

المجلد التاسع - العدد الأول (يناير، فبراير، مارس) 2008

1

الافتتاحية

تكنولوجيا الجيل الثاني للويب
web 2.0 .. ماهي ؟

د. زين عبد الهادي

أوراق العمل

- قواعد البيانات القانونية

د. رؤوف هلال

- المبادئ الكبرى للحكومة الإلكترونية

د. عمر محمد بن يونس

- معضلات البحث في اللغة العربية

أ.د. محمد علي سلامة

- واحة مكتبات . نت

أ. عيبر أحمد

ملف العدد

- أمن المعلومات

م. ممدوح الشحات صقر

IPIS.COM

إيبيس . كوم

مستشار التحرير

أ.د فتحي عبد الهادي

رئيس التحرير

د. زين عبد الهادي

مدير التحرير

د. رؤوف هلال

مراجعة

أ. شريف السيد

IPIS.COM

إيبيس . كوم

ص.ب.: 647 الأورمان

12612 - الجيزة

جمهورية مصر العربية

33832836 : ت/ ف

35839668 : ت

0101816656 : محمول

0106630770 :

www.ipisegypt.com

helal_raouf@hotmail.com

birooahmed@hotmail.com

January, February, March 2008

تابع معنا

أحدث التطبيقات التكنولوجية في المكتبات ومراكز المعلومات

مكتبات. نت

قائمة المحتويات

الاستراتيجية: تكنولوجيا الجيل الثاني للويب web 2.0... ما هي؟

د. زين عبد الهادي ————— 3

أمن المعلومات

م. ممدوح الشحات صقر ————— 4

قواعد البيانات القانونية

د. رؤوف هلال ————— 21

المبادئ الكبرى للحكومة الإلكترونية

د. عمر محمد بن يونس ————— 25

معضلات البحث في اللغة العربية

أ.د. محمد علي سلامة ————— 35

واحة مكتبات. نت

أ. عيبر أحمد ————— 40

نشرة غير دورية تصدر
مؤقتاً تهتم بتكنولوجيا
المكتبات والنظم الآلية
والإنترنت واستخداماتها
في المكتبات العربية

مستشار التحرير

أ.د. محمد لحي عبد الهادي
وكيل كلية الآداب جامعة القاهرة-السابق
واساذ للمكتبات والمعلومات

رئيس التحرير

د. زين الدين عبد الهادي
رئيس قسم المكتبات والمعلومات
جامعة حلوان
zhady41@arado.org.eg

مدير التحرير

د. رؤوف هلال
مدرس المكتبات والمعلومات
كلية الآداب جامعة عين شمس
helal_raouf@hotmail.com

مراجعة

أ. شريفة السيد
مسؤول النشاط الثقافي
دار الكتب المصرية
Shersifa_elsayed@yahoo.com

توزيع

إيبيس.كوم
القاهرة

صدر العدد الأول في يناير
2000

الافتتاحية:

تكنولوجيا الجيل الثاني للويب web 2.0 ... ما هي؟

د. زين عبد الهادي

Zhady41@arado.org.eg

البشر في الموسوعة بدلاً من محررين معينهم، واعتماد ثقافة (الويكي) wiki في بناء المواقع على شبكة الإنترنت، وكذلك ظهرت تكنولوجيا رفع أداء محركات البحث search engine optimization، والتحول من صناعة النشر publishing إلى حرية الاشتراك في النشر participation، وكذلك التحول من ظاهرة الصفحات الشخصية Personnel websites إلى ظهور ما يعرف بالدونات Blogs والتي كانت سبباً في الانتشار السريع للمواقع الشخصية عبر الإنترنت من خلال استضافتها من قبل الشركات العملاقة التي تعمل عبر الويب.

لاشك أن الجيل الثاني للويب قد ترك تأثيرات كبيرة على قضايا البحث والنشر والخدمات على شبكة الإنترنت، ولعل ظهور الجيل الثاني للمكتبات Library 2.0 واحدة من مخرجات الجيل الثاني للويب، لكن السؤال كيف أثر الجيل الثاني للويب على نظم المكتبات وخدماتها؟

زين

يعد

أو رايلي O'reilly أول من أشار إلى مصطلح الجيل الثاني للويب web2.0 وفي مقال له شهير على شبكة الإنترنت بعنوان: what is web 2.0 أشار إلى أهم الفروقات بين تكنولوجيا الجيل الأول للويب، وتكنولوجيا الجيل الثاني لها، حيث أشار إلى أربعة عشر فرقاً بين الجيلين لعل أشهر هذه الفروقات جاءت من ثلاثة أدوات علمية ظهرت على الإنترنت خلال السنوات السبع الماضية يأتي على رأسها تأثير محرك البحث جوجل ثم تأثير موسوعة ويكيبيديا، وأخيراً ظاهرة الدونات أو البلوجز، حيث أثرت هذه الظواهر على تكنولوجيا الإنترنت ككل، بل أصبح الأمر مرتبطاً بمنتجات جوجل نفسها مثل Google scholar والغريب أن جوجل نفسها تعترض على الربط بين اسمها وبين التكنولوجيا المستخدمة، على أية حال أثرت جوجل تأثيراً عريضاً في القضايا المتعلقة بالويب وعلى سبيل المثال في اعتماد تكنولوجيا استشهاد المواقع والصفحات ببعضها البعض بدلاً من استخدام مدى تكرار المصطلح في الصفحات، وكذلك الموسوعة المعروفة باسم الويكيبيديا wikipedia بدلاً للموسوعة البريطانية على الإنترنت Online Britannica، أي الاعتماد على مشاركة كل

أمن المعلومات

م. ممدوح الشحات صقر

• أمن نظم المعلومات

يشمل هذا المساق المفاهيم الأساسية لأمن نظم المعلومات وأهدافه في عصر الاتصالات والإنترنت، أساليب تشفير البيانات، الشبكة الخاصة الافتراضية، حواجز النار، أمن الإنترنت، البريد الإلكتروني المحمي والسياسات الإدارية لأمن نظم المعلومات

مقدمة

تحدث تكنولوجيات المعلومات والاتصال ثورة تمس القطاع الاقتصادي، السياسي، الاجتماعي والثقافي، في نفس أهمية الثورات السابقة. وتعتمد هذه الثورة على المعلومة التي تركز عليها المعرفة البشرية. وتسمح التكنولوجيات الحديثة للمعلومات برصد هذه الأخيرة معالجتها وتوزيعها على اختلاف أوعيتها المكتوبة، الموثية والمسموعة، ذلك بالغالب على عائق حجم المعلومات والتقليص من الوقت اللازم لتوزيعها.

أدت هذه التكنولوجيات إلى طريقة عمل جديدة سهلت ميلاد مفهوم جديد وهو مفهوم مجتمع المعلومات الذي يرمي إلى الاستغلال الكثيف والأمثل للمعلومات في شتى مجالات الحياة. يعتبر هذا المجتمع ولید التقارب التكنولوجي بين المعلوماتية وتكنولوجيات الاتصال. وقد فتح أبواب التفاعل بين عدة متعاملين على المستوى العالمي الذين يقومون بتبادل للمعلومات عبر الشبكة العنكبوتية الانترنيت.

ومن خلال هذا الانفتاح الواسع في مجال الاتصالات ونقل المعلومات وجب علينا معرفة كيف نحافظ على هذه المعلومات المنقولة من جهة لأخرى ومن هنا نشأ مفهوم ومصطلح "أمن المعلومات"

يعتمد تعريف الأمن إلى حد كبير على السياق، لأن كلمة الأمن تشير إلى طيف واسع من المجالات ضمن وخارج حقل تقنية المعلومات. قد نتكلم مثلاً عن الأمن عند توصيف الإجراءات الوقائية على الطرق العامة أو عند استعراض نظام حاسوبي جديد يتمتع بمناعة عالية ضد فيروسات البرمجيات. لقد تم تطوير أنظمة عدة لمعالجة الجوانب المختلفة لفهوم الأمن.

١. ما هو أمن المعلومات؟

لكي نستمكن من استيعاب مفهوم أمن المعلومات لا بد من استعراض السياق التاريخي لتطور هذا المفهوم.

لقد ظل هذا المجال من الأمن حتى أواخر السبعينيات معروفاً باسم أمن الاتصالات Communication Security COMSEC والذي حددته توصيات

أمن أنظمة المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة بما يلي:

المعايير والإجراءات المستخدمة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات.

تضمنت النشاطات المحددة لأمن الاتصالات COMSEC أربعة أجزاء هي: أمن التشفير Cryptosecurity، أمن النقل Transmission Security، أمن الإشعاع Emission Security والأمن الفيزيائي Physical Security. كما تضمن تعريف أمن الاتصالات خاصيتين تتعلقان بموضوع هذه الوحدة: السرية والتحقق من الهوية.

1.1 السرية CONFIDENTIALITY

التأكيد بأن المعلومات لم تصل لأشخاص، عمليات أو أجهزة غير مخولة بالحصول على هذه المعلومات (الحماية من إفشاء المعلومات غير المرخص). التأكيد بأن المعلومات لن

1.2 التحقق من الهوية

إجراء أمني للتأكد من صلاحية الاتصال، الرسالة أو المصدر أو وسيلة للتحقق من صلاحية شخص ما لاستقبال معلومات ذات تصنيف محدد (أو التحقق من مصدر هذه المعلومات).

بدأت في الثمانينيات مع النمو المضطرد للحاسبات الشخصية حقبة جديدة من الأمن: أمن الحواسيب (Computer Security (COMPUSEC والتي حددتها توصيات أمن أنظمة المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة بما يلي:

"المعايير والإجراءات التي تضمن سرية، كمال وتوفر مكونات أنظمة المعلومات بما فيها التجهيزات، البرمجيات، البرمجيات المدمجة firmware والمعلومات التي تتم معالجتها، تخزينها ونقلها". تضمن أمن الحواسيب الشخصية خاصيتين إضافيتين تتعلقان بموضوع هذه الوحدة: الكمال والتوفر.

1.3 الكمال INTEGRITY

تعكس جودة أي نظام للمعلومات مدى صحة ووثوقية نظام التشغيل، التكامل المنطقي للتجهيزات والبرمجيات التي توفر آليات الحماية ومدى تناغم بنى المعلومات مع البيانات المخزنة.

1.4 التوفر AVAILABILITY

الوصول الموثوق إلى البيانات وخدمات المعلومات عند الحاجة إليها من قبل الأشخاص المخولين بذلك. لاحقاً وفي التسعينات من القرن الماضي تم دمج مفهومي الأمن (أمن الاتصالات وأمن الحواسيب) لتشكيل ما أصبح يعرف باسم (أمن أنظمة المعلومات Information Systems Security INFOSEC). يتضمن مفهوم أمن أنظمة المعلومات الخصائص الأربعة المعروفة مسبقاً ضمن مفاهيم أمن الاتصالات وأمن الحواسيب: السرية، التحقق من الهوية، الكمال والتوفر، كما أضيف إليها خاصية جديدة: مكافحة الإنكار.

1.5. مكافحة الإنكار (المؤولية) Non-repudiation

التأكيد بأن مرسل البيانات قد حصل على إثبات يوصل البيانات إلى المرسل إليه وبأن المستقبل قد حصل على إثبات لشخصية المرسل مما يمنع احتمال إنكار أي من الطرفين بأنه قد عالج هذه البيانات.

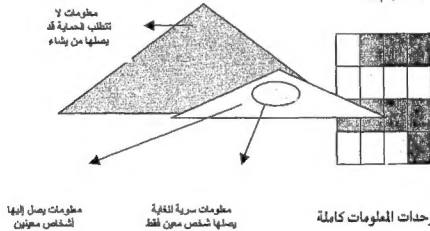
2. هل تحتاج أية معلومات عناصر الحماية ذاتها وبذات القدر؟؟

(منطقات خطة حماية المعلومات)

إن ضمان عناصر أمن المعلومات كلها أو بعضها يعتمد على المعلومات محل الحماية واستخداماتها وعلى الخدمات المتصلة بها، فليس كل المعلومات تتطلب السرية وضمان عدم الإفشاء، وليس كل المعلومات في منشأة واحدة بذات الأهمية من حيث الوصول لها أو ضمان عدم العبث بها، لهذا تنطلق خطط أمن المعلومات من الإجابة عن سلسلة تساؤلات متتالية :-

✓ **التساؤل الأول :-** ما الذي نريد أن نحميه؟؟ وإجابة هذا التساؤل تحدد تصنيف البيانات والمعلومات من حيث أهمية الحماية، إذ تصنف المعلومات تبعاً لكل حالة على حدة، من معلومات لا تتطلب الحماية، إلى معلومات تتطلب حماية قصوى (انظر شكل 1).

شكل رقم 1



✓ **التساؤل الثاني :-** ما هي المخاطر التي تتطلب هكذا حماية؟؟ وتبدأ عملية تحديد المخاطر بتصور كل خطر قد يمس المعلومات محل الحماية أو يهدد أمنها، ابتداءً من قطع مصدر الكهرباء عن الكمبيوتر وحتى مخاطر اختراق النظام من الخارج بواحد أو أكثر من وسائل الاختراق عبر نقاط الضعف، مروراً بإساءة الموظفين استخدام كلمات السر العائدة لهم، ويصير إلى تصنيف هذه المخاطر ضمن قوائم تبعاً لأساس التصنيف، فتصنف كمخاطر من حيث مصدرها ومن حيث وسائل تنفيذها، ومن حيث غرض المتسببين بهذه المخاطر، ومن حيث أثرها على نظام الحماية وعلى المعلومات محل الحماية. وهو ما سنقف لاحقاً عليه بشكل تفصيلي، ومتى ما تم الانتهاء من هذا التحديد يجري الانتقال إلى التساؤل التالي.

✓ التساؤل الثالث :- كيف يتم توفير الحماية لما نرغب بحمايته من المخاطر التي تم تحديدها (وسائل الحماية) ؟؟ وهنا تجد كل منشأة وكل هيئة طريقته الخاصة في توفير الأمن من المخاطر محل التحديد وبحدود متطلبات حماية المعلومات المخصصة التي تم تحديدها وبحدود إمكانياتها المادية والميزانية المخصصة للحماية، فلا تكون إجراءات الأمن رخوة ضعيفة لا تكفل الحماية وبالمقابل لا تكون مبالغاً بها إلى حد يؤثر على عنصر الأداء في النظام محل الحماية، إذ لو تصورنا شخصاً أراد حماية النقود الموجودة في منزله، فإنه من المقبول وضعها مثلاً في قاعة حديدية ووضع حديد حماية مثلاً على نوافذ المنزل، أو وضع جرس إنذار لأي اقتحام للمنزل وربما يمكن قبول هذه الوسائل الثلاث لتوفير الأمن من أنشطة سرقة هذا المال لكن ليس منطقياً بل مبالغاً فيه أن يحمي هذا الشخص ماله بأن يضع حراساً (أشخاصاً) على منزله، ويضع صواعق كهربائية على الأسوار الخارجية، ومن ثم يضع حديد حماية على الأبواب والنوافذ، ويضيف إلى ذلك جرس إنذار لكل نقطة في المنزل، فإذا ما دخلنا إلى المنزل وجدنا كاميرات مراقبة عند كل نقطة، ووجدنا بعدها أن الغرفة التي تحتوي القاعة الحديدية لا يسمح بالدخول إليها إلا بعد تجاوز إجراءات تعريف خاصة بكباقة تعريف أو رقم سري على الأقفال أو غير ذلك، فإذا ما دخلنا الغرفة وجدنا أننا لسنا أمام قاعة حديدية عادية، وإنما خزانة حفظ تفتح بقليل وفتي أو ساعة وقتية، أو تفتح بمفتاحين أو أكثر وبأرقام سرية متعددة أو غير ذلك من أنماط القاصات المعقدة بل ووجدنا أن فتحها يتطلب ابتداء إلغاء جرس إنذار خاص بالقاعة نفسها . أن هكذا حماية لا يمكن أن تكون مقبولة، لأنها ببساطة تجعل عملية حصول الشخص نفسه على بعض المال من بين نقوده عملية معقدة قد تدفعه لاحقاً إلى إهمال كل إجراءات الأمن هذه فيكون أكثر عرضة للسرقة من غيره، وهذا ما نسميه التأثير على صحة الأداء وفعايليته . وفي بيئة المعلومات، فمن الطبيعي مثلاً أن نضع على جهاز الكمبيوتر الشخصي كلمة سر للولوج إلى الملفات الهامة أو حتى للنظام كله وإن لا نعطي الكلمة لأحد، وإن نضع برنامجاً أو أكثر لمقاومة الفيروسات الإلكترونية الضارة، ونراعي إجراءات مقبولة في حماية الدخول إلى شبكة الإنترنت والتأكد من مصدر البريد الإلكتروني مثلاً . فإذا كان الكمبيوتر خاص بذاكرة أو منشأة ويضم بيانات هامة ومصنف أنها سرية، كان لزاماً زيادة إجراءات الأمن، فمثلاً يضاف للنظام جدران نارية تحد من دخول أشخاص من الخارج وتضع اعتداءات منظمة قد يتعرض لها النظام أو الموقع المعلوماتي، وإذا كان النظام يتبادل رسائل إلكترونية يخشى على بياناتها من الإفشاء، تكون تقنيات التشفير مطلوبة بالقدر المناسب . لكن لا يقبل مثلاً على جهاز كمبيوتر خاص غير مرتبط بشبكة عامة أن توضع أنواع متعددة من الجدران النارية، أو أن يوضع على أحد مواقع الإنترنت وسائل تعريف متعددة لشخص المستخدم، ككلمة السر والبصمة الإلكترونية والبصمة الصوتية، وإن يخضع نظام الموقع إلى عدد مبالغ به من الفلترات والجدران النارية، وتشفير طويل المدى لكافة البيانات الموجودة عليه والمتبادلة عبره، وأيضاً لا يقبل موقع أمني يضم بيانات سرية للغاية مجرد الاكتصاع على كلمة سر للدخول للنظام .

بمعنى أن إجراءات الحماية تنطلق من احتياجات الحماية الملائمة، فإن زادت عن حدها أمنت ذات اثر سلبي على الأداء، فاصبح الموقع أو النظام بطيئا وغير فاعل في أداء مهامه الطبيعية، وان نقصت عن الحد المطلوب، ازدادت نقاط الضعف واصبح اكثر عرضة للاختراق الداخلي والخارجي . فإذا فرغنا من اختبار وسائل الحماية التقنية واستراتيجياتها الإدارية والأدائية الملائمة، انتقلنا بعدئذ إلى التساؤل الأخير.

✓ التساؤل الرابع :- ما العمل إن تحقق أي من المخاطر رغم وسائل الحماية ؟؟ وإجابة هذا التساؤل هو ما يعرف بخطة مواجهة الأخطار عند حصولها، وتتضمن مراحل متتالية، تبدأ من مرحلة الإجراءات التقنية والإدارية والإعلامية والقانونية اللازمة عند حصول ذلك، ومرحلة إجراءات التحليل لطبيعية المخاطر التي حصلت وسبب حصولها وكيفية منع حصولها لاحقا . وأخيراً إجراءات التعافي والعودة إلى الوضع الطبيعي قبل حصول الخطر مع مراعاة تنفيذ ما أظهره التحليل عن كيفية حصول المخاطر وضمان عدم حصولها .

إذن، وفي الوقت الذي تتطلب بعض المعلومات كالتصلة بالأمن القومي والأسرار العسكرية مثلا إيلاء عنصري السرية والتكاملية أقصى درجات الاهتمام، نجد بالنسبة للبنوك انه إضافة للعنصرين المتقدمين يتعين بالنسبة للنظام نفسه إيلاء عنصر الاستمرارية ذات القدر من الأهمية، فإن عملت المصارف في حقل البنوك الإلكترونية أو الخدمات المصرفية الإلكترونية عن بعد، كان عنصر عدم الإنكار بنفس أهمية بقية العناصر . ونجد أن مواقع الإنترنت مثلا تتطلب إيلاء عنصر الاستمرارية الأهتمام الأكبر، في حين أن مواقع التجارة الإلكترونية من بين مواقع الإنترنت تتطلب الحرص على توفير عناصر الحماية الأربعة بنفس القدر والأهمية إذ تحتاج ضمان السرية، وتحديدًا بالنسبة للبيانات الخاصة بالزبائن كأرقام بطاقات الائتمان، وتتطلب التكاملية والسلامة بالنسبة للبيانات المتبادلة عبر الرسائل الإلكترونية بين الزبون والموقع، فلا يصل أمر الشراء مثلا وقد لحقه تغيير أو تحريف ما، وتتطلب استمرارية الموقع في تقديم خدماته وقدرته الزبون على الولوج إليه طوال وقت سريان عملية التصفح والشراء بل وفي أي وقت يريد للدخول إلى الموقع، وتتطلب ضمان عدم إنكار الزبون إن التصرف الذي أجراه على الموقع (كطلب الشراء) قد صدر عنه أو إنكار الموقع نفسه انه تعاقد مع الزبون في شأن ما .

2.1. أين تتجه المخاطر والاعتداءات في بيئة المعلومات ؟؟

تطال المخاطر والاعتداءات في بيئة المعلومات أربعة مواطن أساسية هي مكونات تقنية المعلومات في احدث تجلياتها :-

✓ الأجهزة :- وهي كافة المعدات والأدوات المادية التي تتكون منها النظم، كالشاشات والطابعات ومكوناتها الداخلية ووسائل التخزين المادية وغيرها .

✓ البرامج :- وهي الأوامر المرتبة في نسق معين لإنجاز الأعمال، وهي إما مستقلة عن النظام أو مخزنة فيه .

✓ المعطيات :- أنها الدم الحي للأنظمة، وما سيكون محلا لجرائم الكمبيوتر كما سرى، وتشمل كافة البيانات المدخلة والمعلومات المستخرجة عقب معالجتها، وتمتد بمعناها الواسع للبرمجيات المخزنة داخل النظم . والمعطيات قد تكون في طور الإدخال أو الإخراج أو التخزين أو التبادل بين النظم عبر الشبكات، وقد تخزن داخل النظم أو على وسائط التخزين خارجة .

✓ الاتصالات :- وتشمل شبكات الاتصال التي تربط أجهزة التقنية بعضها بعضا محليا ونطاقيا ودوليا، وتتيح فرصة اختراق النظم عبرها كما أنها بذاتها محل للاعتداء وموطن من مواطن الخطر الحقيقي.

3. ما هي عمليات المعلومات الرئيسية المتصلة بأمن المعلومات؟؟

تتعدد عمليات التعامل مع المعلومات في بيئة النظم وتقنيات المعالجة والاتصال وتبادل البيانات، ولكن يمكن بوجه عام تحديد العمليات الرئيسية التالية :-

3.1. تصنيف المعلومات Information classification :-

وهي عملية أساسية لدى بناء أي نظام أو في بيئة أي نشاط يتعلق بالمعلومات وتختلف التصنيفات حسب المنشأة مدار البحث، فمثلا قد تصنف المعلومات إلى معلومات متاحة، وموثوقة، وسرية، وسرية للغاية أو قد تكون معلومات متاح الوصول إليها وأخرى محظور الوصول إليها وهكذا .

3.2. التوثيق Documentation :-

وتتطلب عمليات المعلومات أساسا اتباع نظام توثيق خطي لتوثيق بناء النظام وكافة وسائل المعالجة والتبادل ومكوناتها . وبشكل رئيس فإن التوثيق لازم وضروري لنظام التعريف والتحويل، وتصنيف المعلومات، والأنظمة التطبيقية . وفي إطار الأمن، فإن التوثيق يتطلب أن تكون استراتيجية أو سياسة الأمن موثقة ومكتوبة وأن تكون إجراءاتها ومكوناتها كاملة محل توثيق، إضافة إلى خطط التعامل مع المخاطر والحوادث، والجهات المسؤولة ومسؤولياتها وخطط التعافي وإدارة الأزمات وخطط الطوارئ المرتبطة بالنظام عند حدوث الخطر .

3.3. المهام والواجبات الإدارية والشخصية Administration and Personnel

Responsibilities

إن مهام المتصلين بنظام أمن المعلومات تبدأ في الأساس من حسن اختيار الأفراد المؤهلين وعمق معارفهم النظرية والعملية، على أن يكون مدركا أن التأهيل العملي يتطلب تدريباً متواصلاً ولا يقف عند حدود معرفة وخبرة هؤلاء لدى تعيينهم، وبشكل رئيس فإن المهام الإدارية أو التنظيمية تتكون من خمسة عناصر أو مجموعات رئيسية :- تحليل المخاطر، وضع السياسة أو الاستراتيجية، وضع خطة الأمن، وضع البناء التقني الأمني-توظيف الأجهزة والعدات والوسائل، وأخيراً تنفيذ الخطط والسياسات .

3.4. وسائل التعريف والتوثيق من المستخدمين وحدود صلاحيات الاستخدام

Identification and Authorization :-

إن الدخول إلى أنظمة الكمبيوتر وقواعد البيانات ومواقع المعلوماتية عموماً، يمكن تقييده بالعديد من وسائل التعرف على شخصية المستخدم وتحديد نطاق الاستخدام، وهو ما يعرف بأنظمة التعريف والتحويل Identification and Authorization systems . والتعريف أو الهوية مسألة تتكون من

خطوتين، الأولى وسيلة التعريف على شخص المستخدم، والثانية قبول وسيلة التعريف أو ما يسمى التوثيق من صحة الهوية المقدمة

ووسائل التعريف تختلف تبعاً للتقنية المستخدمة، وهي نفسها وسائل أمن الوصول إلى المعلومات أو الخدمات في قطاعات استخدام النظم أو الشبكات أو قطاعات الأعمال الإلكترونية، وبشكل عام، فإن هذه الوسائل تنوزع إلى ثلاثة أنواع :-

1 - شئ ما يملكه الشخص مثل البطاقة البلاستيكية أو غير ذلك .

2- شئ ما يعرفه الشخص مثل كلمات السر أو الرمز أو الرقم الشخصي غير ذلك .

3- شئ ما يرتبط بذات الشخص أو موجود فيه مثل بصمة الإصبع أو بصمة العين والصوت وغيرها .

وتعد وسائل التعريف والتوثيق الأقوى، تلك الوسائل التي تجمع بين هذه الوسائل جميعاً على نحو لا يؤثر على سهولة التعريف وفمايلته في ذات الوقت .

3.5 سجل الأداء Logging :-

تحتوي مختلف أنواع الكمبيوترات نوعاً ما من السجلات التي تكشف استخدامات الجهاز وبرمجياته والنفاذ إليه، وهي ما يعرف بسجلات الأداء أو سجلات النفاذ إلى النظام ، تتخذ سجلات الأداء أهمية استثنائية في حال تعدد المستخدمين وتحديداً في حالة شبكات الكمبيوتر التي يستخدم مكوناتها أكثر من شخص، وفي هذه الحالة تحديداً، أي شبكات المستخدمين، فإن هناك أكثر من نوع من أنواع سجلات الأداء وتوثيق الاستخدامات، كما أن سجلات الأداء تتباين من حيث نوعها وطبيعتها وغرضها، فهناك سجلات الأداء التارخية والسجلات المؤقتة، وسجلات التبادل وسجلات النظام وسجلات الأمن وسجلات قواعد البيانات والتطبيقات وسجلات الصيانة أو ما يعرف بسجلات الأمور التقنية وغيرها.

3.6 عمليات الحفظ Back-up :-

وعمليات الحفظ تتعلق بعمل نسخة إضافية من المواد المخزنة على إحدى وسائط التخزين سواء داخل النظام أو خارجه، وتخضع عمليات الحفظ لقواعد يمتنع أن تكون محددة سلفاً وموثقة ومكتوبة ويجري الالتزام بها لضمان توحيد معايير الحفظ وحماية النسخ الاحتياطية . ويمثل وقت الحفظ، وحماية النسخ الاحتياط، ونظام الترميز والتبويب، وآلية الاسترجاع والاستخدام، ومكان الحفظ وأمنه، وتشفير النسخ التي تحتوي معطيات خاصة وسرية، مسائل رئيسية يمتنع اتخاذ معايير واضحة ومحددة بشأنها .

3.7 وسائل الأمن الفنية ونظام منع الاختراق :-

تتعدد وسائل الأمن التقنية المتعين استخدامها في بيئة الكمبيوتر والإنترنت، كما تتعدد أغراضها ونطاقات الاستخدام وتتخذ الجدران النارية **Firewalls**، إضافة للتشفير **cryptography**، وكذلك نظم

التحكم في الدخول و نظام تحري الاختراق (Intrusion Detection Systems (IDS، وأنظمة وبرمجيات مقاومة الفيروسات أهمية متزايدة، لكنها لا تمثل جميعها وسائل الأمن المستخدمة، بل هي إضافة لوسائل التعريف والتوثيق المتقدم الإشارة إليها تمثل أهم وسائل الأمن التقنية في الوقت

3.8. نظام التعامل مع الحوادث Incident Handling System :-

بغض النظر عن حجم وسائل الأمن التقنية المستخدمة، ومعايير الأمن وإجراءاته المتبعة، فإنه لا بد من توفر نظام متكامل للتعامل مع المخاطر والحوادث والاعتداءات، ويعدو مطلباً رئيساً بالنسبة لمؤسسات الأعمال كما في حالة البنوك والمؤسسات المالية .

وأول ما يتعين إدراكه في هذا الصدد أن التعامل مع الحوادث عملية وليست مجرد مشروع أو خطوة واحدة، بمعنى أنها عملية متكاملة تتصل بأداء متواصل متدرج خاضع لقواعد محددة سلفاً ومتبعة بدقة وانضباط، ومتى ما تم التعامل مع الحوادث على أنها مجرد حالة تنشأ عند الحادث كنا أمام حالة قصور تمثل بذاتها أحد عناصر الضعف في نظام الأمن .

وتختلف مكونات ومراحل وخطوات نظام التعامل مع الحوادث من مؤسسة إلى أخرى تبعا لعوامل عديدة تتعلق بطبيعة الأخطار التي أظهرتها عملية تحليل المخاطر وما أظهرته استراتيجيات الأمن الموضوعة في المؤسسة، وتبعاً للنظام محل الحماية وما إذا كنا نتحدث عن نظم كمبيوتر مغلقة أم مفتوحة أو قواعد بيانات أو شبكات أو مزيج منها وما إذا كنا نتحدث عن نظام خدمة بخصوص أم عن خدمات للعملاء عبر الشبكة خاصة كانت أم دولية وتبعاً لوظيفة التطبيق محل الحماية، إذ تتباين خطوات ومحتوى وهنالك عناصر خطط التعامل مع الحوادث لدى بنوك الإنترنت مثلاً عنها لدى المواقع المعلوماتية، ومع ذلك، وبوجه عام، فإن نظام التعامل مع الحوادث يتكون عادة من ستة مراحل (خطوة فخطوة) هي :-

الإعداد المسبق والتحري والملاحظة الاحتواء والاستئصال، التعافي والعودة للوضع الطبيعي، والمتابعة .

4. ما هي المخاطر والتهديدات ونقاط الضعف وأنواع الهجمات والاعتداءات وأساليبها التقنية ؟

4.1. في المفاهيم والاصطلاحات :-

إن الحدود بين الجريمة والفعل غير الأخلاقي تبدو غير واضحة المعالم في بيئة الكمبيوتر والإنترنت، وتتميز وضبط هذه الحدود هو المسألة الجوهرية لتحديد متى يمكن أن يعد فعل ما جريمة من بين جرائم الكمبيوتر والإنترنت أو أنه مجرد إساءة استخدام لا ينطوي على قصد جرمي وهي المسألة التي أحدثت جدلاً واسعاً في مطلع الستينات وحتى منتصف السبعينات وهي ذات الفترة التي شهدت ميلاد ظاهرة جرائم الكمبيوتر، ومن جديد يعود هذا الجدل بسبب شيوع استخدام الإنترنت وما حملته من أنشطة جديدة لا يزال الخلاف قائماً حول ما إذا كانت جريمة أم أنها مجرد ممارسة غير مقبولة كسلوك أخلاقي لكنها لا ترقى إلى حد الجريمة.

إن غرض هذا التقديم محاولة تقديم تحديد منضبط للاصطلاحات المستخدمة في عالم جرائم الكمبيوتر والإنترنت، لجهة التمييز بين العديد من الاصطلاحات التي يجري الخلط بينها، فثمة فرق بين الجريمة

الإلكترونية، الإرهاب الإلكتروني، حرب المعلومات، المخاطر، الحوادث، نقاط الضعف، والأخطاء، الاختراقات، حرب المعلومات وغيرها .

التهديد Threats : ويعني الخطر المحتمل الذي يمكن أن يتعرض له نظام المعلومات وقد يكون شخصا، كالتجسس أو المجرم المحترف أو الهاكرز المخترق، أو شيئا يهدد الأجهزة أو البرامج أو المعطيات، أو حدثا كالحريق وانقطاع التيار الكهربائي والكوارث الطبيعية .

نقاط الضعف أو الثغرات Vulnerabilities : وتعني عنصر أو نقطة أو موقع في النظام يحتمل أن ينفذ من خلاله المعتدي أو يتحقق بسببه الاختراق فمثلا يعد الأشخاص الذين يستخدمون النظام نقطة ضعف إذا لم يكن تدريبهم كافيا لاستخدام النظام وحمايته، وقد يكون الاتصال بالإنترنت نقطة ضعف مثلا إذا لم يكن مشفرا . وقد يكون الموقع المكاني للنظام نقطة ضعف كأن يكون غير مجهز بوسائل الوقاية والحماية، وبالمعنى فإن نقاط الضعف هي الأسباب المحركة لتحقيق التهديدات أو المخاطر . ويرتبط بهذا الاصطلاح اصطلاح وسائل الوقاية **Countermeasures** : وتعني التكنيك المتبع لحماية النظام ككلمات السر والأقفال ووسائل الرقابة والجدول النارية وغيرها .

أما المخاطر Risks : فإنها تستخدم بشكل مترادف مع تعبير التهديد، مع إنها حقيقة تتصل بأثر التهديدات عند حصولها، وتقوم استراتيجية أمن المعلومات الناجحة على **تحليل المخاطر Risk analysis**، وتحليل المخاطر هي عملية **Process** وليست مجرد خطة محصورة، وهي تبدأ من التساؤل حول التهديدات ثم نقاط الضعف وأخيراً وسائل الوقاية المناسبة للتعامل مع التهديدات ووسائل منع نقاط الضعف .

أما الحوادث Incident :- فهو اصطلاح متسع يشمل المخاطر ويشمل الأخطاء، وهو بالمعنى المستخدم في دراسات أمن المعلومات إبتغية يشير إلى الأفعال المقصودة أو غير المقصودة، ويغطي الاعتداءات والأخطاء الفنية و يتعين أن يحمله على الحوادث غير المقصودة والتي قد تكون مخاطر بفعل الطبيعة ودون عامل قصدي أو تكون أخطاء فنية غير مقصودة .

أما الهجمات Attacks فهو اصطلاح لوصف الاعتداءات بنتائجها أو بموضع الاستهداف، فنقول هجمات إنكار الخدمة، أو هجمات إرهابية، أو هجمات البرمجيات، أو هجمات الموظفين الحاقدة أو الهجمات المزاحية . ويستخدم كاصطلاح رديف للهجمات اصطلاح الاختراقات أو **الإخلالات Breaches** . وهو اصطلاح توصف به مختلف أنماط الاعتداءات التقنية، وبالتالي يكون مرادفا أيضا للاعتداءات .

5. تصنيف الهجمات في ضوء مناطق ومحل الحماية :-

في الحقل التقني، قد نحسم ويتعين أن نحسم البيئة المادية المحيطة بالأجهزة والنظم، وهذا ما يعرف بالحماية المادية، وهذه مستهدفة من أنواع معينة من الاعتداءات والمخاطر . ويتعين أن نحسم المنشأة من المخاطر المتصلة بالموظفين، وبالتالي ثمة اعتداءات تتصل بشؤون الموظفين والأشخاص، وهناك اعتداءات تتصل

بالمعطيات ذاتها ونظم التوصل إليها، وأخيراً ثمة اعتداءات تتعلق بعمليات النظام ذاته، وهذا التصنيف الذي قال به قطاع عريض من الخبراء التقنيين أو الباحثين في حقل أمن المعلومات، لا يمثل تحديداً منضبطاً وإن كان تحديداً يتصف بقدر واسع من الشمولية، ومرد ذلك أن الاعتداء الواحد قد يجد موضعه في طائفة أو أكثر من هذه التقسيمات وبالمعوم، تصنف المخاطر والاعتداءات وفق هذه الرؤيا على النحو التالي :-

أولاً :- خرق الحماية المادية Breaches of Physical security

- **التفتيش في مخلفات التقنية Dumpster diving** ويقصد به قيام المهاجم بالبحث في مخلفات المؤسسة من القمامة والمواد المتروكة بحثاً عن أي شيء، يساعد على اختراق النظام، كالأوراق المدون عليها كلمات السر، أو مخرجات الكمبيوتر التي قد تتضمن معلومات مفيدة، أو الأقراص الصلبة المرسية بعد استبدالها، أو غير ذلك من المواد المكتوبة أو الأقراص أو الملاحظات أو أي أمر يستدل منه على أية معلومة تساهم في الاختراق

- **الالتقاط السلكي Wiretapping** :- والمقصود هنا ببساطة التوصل السلكي للمادي مع الشبكة أو توصيلات النظام لجهة استراق السمع أو سرقة والاستيلاء على المعطيات المتبادلة عبر الأسلاك، وهي أنشطة تتم بطرق سهلة أو معقدة تبعاً لنوع الشبكة وطرق التوصل المادي .

- **استراق الأمواج Eavesdropping on Emanations** : ويتم ذلك باستخدام لواقط تقنية لتجميع الموجات المنبعثة من النظم باختلاف أنواعها كاللتقاط موجات شاشات الكمبيوتر الصوتية أو التقاط الموجات الصوتية من أجهزة الاتصال .

- **إنكار أو إلغاء الخدمة Denial or Degradation of Service** :- والمقصود هنا الإضرار المادي بالنظام لمنع تقديم الخدمة، أما إن كنا نتحدث عن إنكار الخدمة مثلاً على مواقع الإنترنت فإن ذلك يتم عبر تقنيات مختلفة، كضخ الرسائل البريدية الإلكترونية دفعة واحدة لتعطيل النظام .

ثانياً :- خرق الحماية المتعلقة بالأشخاص وشؤون الموظفين Personnel security

Breaches of

تعد المخاطر المتصلة بالأشخاص والموظفين، وتحديد المخاطر الداخلية منها، واحدة من مناطق الاهتمام العالمي لدى جهات أمن المعلومات، إذ ثمة فرصة لأن يحقق أشخاص من الداخل ما لا يمكن نظرياً أن يحققه أحد من الخارج، وتظل أيضاً مشكلة صمويات كشف هؤلاء قائمة إن لم يكن ثمة نظام أداء وصلاحيات يتيح

- **التخفي بانتحال صلاحيات شخص مغووص Masquerading** :- المقصود هنا الدخول إلى النظام عبر استخدام وسائل التعريف العائدة لمستخدم مخول بهذا الاستخدام، كالاستغلال بكلمة سر أحد المستخدمين واسم هذا المستخدم، أو عبر استغلال نطاق صلاحيات المستخدم

- الهندسة الاجتماعية **Social Engineering** ويعتبر هذا الأسلوب ضمن الحماية المادية أحيانا ويرجع إلى أنشطة الحصول على معلومات تهيئ الاقتحام من خلال علاقات اجتماعية، وذلك باستغلال الشخص أحد عناصر النظام- أشخاصه- بإيهامه بأي أمر يؤدي إلى حصول هذا الشخص على كلمة مرور أو على أية معلومة تساعد في تحقيق

- الإزعاج والتحرش **Harassment** :- وهي تهديدات يندرج تحتها أشكال عديدة من الاعتداءات والأساليب، ويجمعها توجيه رسائل الإزعاج والتحرش وربما التهديد والابتزاز أو في أحيان كثيرة رسائل المزاح على نحو يحدث مضايقة وإزعاجا بالفيديو، وليست حكرا على البريد الإلكتروني بل تستغل مجموعات الحوار والأخبار والنشرات الإلكترونية في بيئة الإنترنت والويب

- قرصنة البرمجيات **Software Piracy** وقرصنة البرامج تتحقق عن طريق نسخها دون تصريح أو استغلالها على نحو مادي دون تحويل بهذا الاستغلال، أو تقليدها ومحاكاتها والانتفاع المادي بها على نحو يخل بحقوق المؤلف، وهو نشاط يندرج في حقيقته ضمن طائفة الاعتداءات والمخاطر التي تستهدف البرمجيات عموما، وهو قطاع استقل بذاته من بين قطاعات جرائم الكمبيوتر

ثالثا :- خرق الحماية المتصلة بالاتصالات **Breaches of Communications and Security** والمقصود بهذه الطائفة الأنشطة التي تستهدف المعطيات والبرمجيات ذاتها وتشمل طائفتين :-

• هجمات المعطيات **Data Attacks**

- النسخ غير المصرح به للمعطيات **Unauthorized Copying of Data** :- وهي العملية الشائعة التي تستتبع الدخول غير المصرح به للنظام، حيث يمكن الاستيلاء عن طريق النسخ على كافة أنواع المعطيات، وهنا تشمل البيانات والمعلومات والأوامر والبرمجيات وغيرها .

- تحليل الاتصالات **Traffic Analysis** :- الفكرة هنا ببساطة إن الهجوم ينصب على دراسة أداء النظام في مرحلة التعامل ومتابعة ما يتم فيه من اتصالات وارتباطات بحيث يستفاد منها في تحديد مسلكيات المستخدمين وتحديد نقاط الضعف ووقت الهجوم المناسب وغير ذلك من مسائل يجمعها فكرة الرقابة على حركة النظام بغرض تيسير الهجوم عليه .

- القنوات المخفية **Covert Channels** :- وهي عمليا صورة من صور اعتداءات التخزين، حيث يخفي المتحم معطيات أو برمجيات أو معلومات مستولى عليها كأرقام بطاقات ائتمان في موضع معين من النظام، وتتعدد أغراض الإخفاء، فقد تكون تمهيدا لهجوم لاحق أو تغطية اقتحام سابق أو مجرد تخزين لمعطيات غير مشروعة .

• هجمات البرمجيات **Software Attacks**

- المصادن أو الأبواب الخلفية **Trap Doors** :- الأبواب الخلفية ثغرة أو منفذ في برنامج يتيح للمخترق الوصول من خلاله إلى النظام، إنه ببساطة مدخل مفتوح تماما كالأبواب الخلفية للمنزل الذي ينفذ منه السارق .

الهجمات عبر التلاعب بنقل المعطيات عبر إنفاق النقل Tunneling :- إنفاق النقل في الأصل طريقة تقنية مشروعة لنقل المعطيات عبر الشبكات غير المتوافقة، لكنها تصبح طريقة اعتداء عندما تستخدم حزم المعطيات المشروعة لنقل معطيات غير مشروعة .

- **الهجمات الوقتية Timing attacks** وهي هجمات تتم بطرق تقنية معقدة للوصول غير المصرح به إلى البرامج أو المعطيات، وتقوم جميعها على فكرة استغلال وقت تنفيذ الهجمة متزامنا مع فواصل الوقت التي تفصل العمليات المرتبة في النظام، وتضم في نطاقها العديد من الأساليب التقنية لتفنية الهجوم، منها إساءة استغلال الأوضاع أو الأنماط العادية للأداء والكيفية في النظام **Race conditions** والهجمات غير المتزامنة أو غير التوافقة المتصلة باستغلال ترتيب تنفيذ العمليات الاعتيادية **Asynchronous attacks**.

- **البرمجيات الخبيثة Malicious Code** كالفيروسات **Viruses** وحصان طروادة **Trojan Horses** والدودة الإلكترونية **Warms** والسلامي **Salamis** والقنابل المنطقية **Logic Bombs** :- الجامع المشترك بين هذه البرمجيات أنها برمجيات غارة تستغل للتدمير سواء تدمير النظام أو البرمجيات أو المعطيات أو الملفات أو الوظائف أو تستثمر للقيام بهام غير مشروعة كإنجاز احتيال أو غش في النظام، والحقيقة أنها ليست تسميات مترادفة للفيروسات الشائعة

رابعا :- **الهجمات والمخاطر المتصلة بعمليات الحماية Breaches of Operations Security** وإذا ما أردنا أن نوصف المخاطر المتصلة بعمليات الحماية ذاتها ربما نكون في الحقيقة أمام كافة أنواع المخاطر والهجمات والاعتداءات، لكن من زاوية تقنية ضيقة، يشار إلى خمسة أنواع من الأساليب ضمن هذه الطائفة، بعضها يتصل بالهجمات التي تستهدف نظام أو إستراتيجية الدخول، بعضها يستهدف نظام إدخال ومعالجة والبيانات، وبعضها يصنف كفعل أولي لتحقيق عمليات الدخول غير المصرح به إلى مختلف أنواع الشبكات، وسنشير بإيجاز إلى هذه الأساليب والاعتداءات، مع إيضاح لمسميات أخرى من الأنشطة والأساليب والاعتداءات تتصل باختراق الشبكات تحديدا وبيان لأهم نقاط الضعف وفقا لما توصلت إليه أدلة أمن المعلومات المتخصصة جراء الدراسات البحثية :-

- **العبث (الغش) بالبيانات Data Diddling** :- ويستهدف هذا الهجوم أو الاعتداء تغيير البيانات أو إنشاء بيانات وهمية في مراحل الإدخال أو الاستخراج، ويتم في الحقيقة بعشرات الأنماط والأساليب التقنية، جامعا السباح بأمن وحماية مرحلة إدخال البيانات أو استخراجها .
- **خداع بروتوكول الإنترنت IP Spoofing** (التخفي باستغلال بروتوكولات النقل) :- الحقيقة أن اصطلاح **Spoofing** لا يعني التخفي، فهو اصطلاح يتعلق بالغش والخداع والإيهام والتقليد والمحاكاة والسخرية، لكن استخدامه الشائع الآن يتعلق بهجمات فيروسات الإنترنت، والفكرة هنا قريبة من فكرة التخفي التي عرضنا لها أعلاه عندما يتخذ شخص أو ينتحل صفة مستخدم آخر مخول

بالاستخدام، لكن الفرق هنا، إننا نتحدث عن وسيلة تقنية بحتة، بحيث يقوم المهاجم عبر هذه الوسيلة بتزوير العنوان المرفق مع حزمة البيانات المرسلة بحيث يظهر للنظام طبعاً المعتمد في تبادل المعطيات على بروتوكولات النقل وأهمها هنا بروتوكول الإنترنت الأساسي— على أنه عنوان صحيح مرسل من داخل الشبكة، بحيث يسمح النظام لحزمة البيانات بالمرور باعتبارها حزمة مشروعة (إن جاز التعبير).

— تضم كلمات السر (جمعها والتقاطها) **Password Sniffing** :— وإذا كانت أنشطة الاعتداء التي تتم باستعمال كلمات السر كانت تتم غالباً فيما سبق عن طريق تخمين كلمات السر مستفيدة من ضعف الكلمات عموماً وشيوع اختيار الأفراد لكلمات سهلة تتصل بمحيطهم الأسرى أو محيط العمل أو حياتهم الشخصية، فإن الجديد استخدام برمجيات يمكنها تضم أو التقاط كلمات السر خلال تجوالها في جزء من الشبكة أو أحد عناصرها ومراقبتها ومتابعتها لحركة الاتصال على الشبكة، بحيث يقوم هذا البرنامج من حيث الأصل بجمع أول 128 بايت أو أكثر— مثلاً— من كل اتصال بالشبكة التي تجري مراقبتها وتتبع حركة الاتصال عليها، وعندما يطبع المستخدم كلمة السر أو اسم المستخدم، فإن البرنامج (الشمام) يجمع هذه المعلومات وينسخها إضافة إلى أن أنواع من هذه البرامج تجمع المعلومات الجزئية وتعيد تحليلها ويطبعها معاً كما تقوم بعضها بإخفاء أنشطة الالتقاط بعد قيامها بمهمتها .

— المسح والنسخ **Scanning** :— وهو أسلوب يستخدم فيه برنامج (الماسح— **ware dialer demon dialer processes**) الذي هو برنامج احتمالات يقوم على فكرة تغيير التركيب أو تبديل احتمالات المعلومة، ويستخدم تحديداً بشأن احتمالات كلمة السر أو رقم هاتف المودم أو نحو ذلك، وبأبسط نمط فيه عندما تستخدم قائمة الاحتمالات لتغيير رقم الهاتف يسمح قائمة أرقام كبيرة للوصول إلى أحدها الذي يستخدم مودم للاتصال بالإنترنت، أو إجراء مسح لاحتمالات عديدة لكلمة سر للوصول إلى الكلمة الصحيحة التي تمكن المخترق من الدخول للنظام، ومن جديد فإن هذا أسلوب تقني يعتمد واسطة تقنية هي برنامج (الماسح) بدلاً من الاعتماد على التخمين البشري .

— هجومات استغلال المزايا الإضافية **Excess Privileges** :— الفكرة هنا تتصل بواحد من أهم استراتيجيات الحماية، فالأصل أن مستخدم النظام— تحديداً داخل المؤسسة— محدد له نطاق الاستخدام ونطاق الصلاحيات بالنسبة للنظام، لكن ما يحدث في الواقع العملي أن مزايا الاستخدام يجري زيادتها دون تقدير لمخاطر ذلك أو دون علم من الشخص نفسه إنه يحتل مزايا تتجاوز اختصاصه وروغبته، في هذه الحالة فإن أي مخترق للنظام لن يكون فقط قادراً على تدمير أو التلاعب ببيانات المستخدم الذي دخل على النظام من خلال اشتراكه أو عبر نقطة الدخول الخاصة به، أنه ببساطة سيتمكن من تدمير مختلف ملفات النظام حتى غير المتصلة بالمدخل الذي دخل منه لأنه استثمار المزايا الإضافية التي يتمتع بها المستخدم الذي تم الدخول عبر مدخله .

6. تصنيف المخاطر تبعا لموضع المعلومة من النظام وتبعا للواسطة التقنية

إن المعلومات تتعرض للعديد من المخاطر في مراحل الجمع والمعالجة والاسترجاع- سواء قراءة أو طباعة أو تنزيل- وفي مرحلة النقل والتبادل وفي مرحلة التخزين، وهذه المخاطر تختلف تبعا لهذه العمليات ذاتها، إذ لكل مرحلة مخاطرها ووسائل حمايتها الخاصة . وبشكل عام فإن أغلب قوائم تصنيف المخاطر تعتمد معيار موضع المعلومات من النظام. ومن ذلك مثلا قائمة منظمة الشرطة العالمية / الإنترنت التي تعرضها تاليا والتي تقوم من ضمن معيارها - على تبويب المخاطر تبعا لموضع المعلومة أولا حيث تصنف إلى ثلاثة طوائف :-

- طائفة المخاطر التي تتعرض لها المعلومات في مرحلة خلق واسترجاع وتعديل وإلغاء المعلومات، وجامعها وجود المعلومات داخل النظام .

- READ/CREATE/MODIFY/DELETE refers to information (data and software) inside the computer system

- طائفة المخاطر التي تتعرض لها المعلومات في مرحلة النقل، أي التبادل بين أنظمة الكمبيوتر .

- TRANSPORT refers to information (data and software) 'transported' via a network or on media

- طائفة المخاطر التي تتعرض لها المعلومات في مرحلة التخزين على وسائط خارج النظام .

- STORE refers to information (data and software) when it is stored on computer media and taken out of the computer system. (I.e. back-up tapes/diskettes)

كما أن المخاطر تختلف تبعا لواسطة تقنية المعلومات مدار البحث، فليست مخاطر الشبكات والدخول عبرها إلى نظم الكمبيوتر، كمخاطر الكمبيوترات غير المرتبطة بالشبكة، ومخاطر الإنترنت أو الأكسفرانت تختلف عن مخاطر الإنترنت، وحماية الكمبيوتر الشخصي يختلف عن حماية السيرفرات العملاقة التي تدير شبكة معلومات وتتحكم بها، ومخاطر مواقع التجارة الإلكترونية والأعمال الإلكترونية على الشبكة تختلف عن مخاطر موقع معلوماتي ليس أكثر من (بروفایل) إعلاني، كما أن ثغرات ونقاط الضعف تختلف تبعا للوسيلة أو الواسطة أو التقنية مدار البحث . ومن هذه الزاوية ثمة :- مخاطر وثغرات الشبكات سواء المحلية أو المفاطعية أو الدولية- الإنترنت . وكذلك مخاطر وتهديدات الأجهزة بأنواعها (الكمبيوترات الكبرى الرئيسية، الشخصية، المحمولة .. الخ مخاطر تطلال المعطيات والبرمجيات بمختلف مناطق وجودها داخل وخارج النظام.

وهذا هو المعيار الثاني الذي يمثل إلى جانب معيار موضع المعلومة الأساس في قائمة المخاطر والأساليب التقنية للاعتداء والمحددة من قبل جهات عديدة لتنفيذ القانون منها الشرطة الدولية (الإنترپول).

7. ما هي وسائل الأمن التقنية ؟؟

7.1. وسائل الأمن الشائعة

وسائل أمن المعلومات هي مجموعة من الآليات والإجراءات والأدوات والمنتجات التي تستخدم للوقاية من أو تقليل المخاطر والتحديات التي تتعرض لها الكمبيوترات والشبكات وبالعموم نظم المعلومات وقواعدها . وكما أوضحنا، فإن وسائل الأمن متعددة من حيث الطبيعة والغرض، لكن يمكننا بشكل أساسي تصنيف هذه الوسائل في ضوء غرض الحماية إلى الطوائف التالية :-

- مجموعة وسائل الأمن المتعلقة بالتعريف بشخص المستخدم وموثوقية الاستخدام ومشروعيته **Identification and authentication**، وهي الوسائل التي تهدف إلى ضمان استخدام النظام أو الشبكة من قبل الشخص المخول بهذا الاستخدام، وتضم هذه الطائفة كلمات السر بأنواعها، والبطاقات الذكية المستخدمة للتعريف، ووسائل التعريف البيولوجية التي تعتمد على سمات معينة في شخص المستخدم متصلة ببنائه البيولوجي، ومختلف أنواع المنتجات التي تزود كلمات سر آتية أو وقتية متغيرة إلكترونياً، والمفاتيح المشفرة، بل تضم هذه الطائفة ما يعرف بالأقفال الإلكترونية التي تحدد مناطق النفاذ

- مجموعة الوسائل المتعلقة بالتحكم بالدخول والنفاذ إلى الشبكة **Access control** وهي التي تساعد في التأكد من أن الشبكة ومصادرها قد استخدمت بطريقة مشروعة، وتشمل من بين ما تشمل الوسائل التي تعتمد على تحديد حقوق المستخدمين، أو قوائم أشخاص المستخدمين أنفسهم، أو تحديد المزايا الاستخدامية أو غير ذلك من الإجراءات والأدوات التي تتيح التحكم بمشروعية استخدام الشبكة ابتدأً .

- مجموعة الوسائل الهادفة لحماية التكاملية (سلامة المحتوى) **Data and message integrity** وهي الوسائل المغاط بها ضمان عدم تعديل محتوى الميطات من قبل جهة غير مخولة بذلك، وتشمل من بين ما تشمل تقنيات الترميز والتوقيع الإلكترونية وبرمجيات تحري الفيروسات وغيرها.

- مجموعة الوسائل المتعلقة بمنع الإنكار (إنكار التصرفات الصادرة عن الشخص) **Non-repudiation**، وتهدف هذه الوسائل إلى ضمان عدم قدرة شخص المستخدم من إنكار أنه هو الذي قام بالتصرف، وهي وسائل ذات أهمية بالغة في بيئة الأعمال الإلكترونية والتعاقدات على الخط، وترتكز هذه الوسائل حالياً على تقنيات التوقيع الإلكتروني وشهادات التوثيق الصادرة عن طرف ثالث.

- وسائل مراقبة الاستخدام وتتمتع سجلات النفاذ أو الأداء (الاستخدام) **Logging and Monitoring**، وهي التقنيات التي تستخدم لمراقبة العاملين على النظام لتحديد الشخص الذي قام بالعمل المعين في وقت معين، وتشمل كافة أنواع البرمجيات والسجلات الإلكترونية التي تحدد الاستخدام.

- إيضاح موجز حول أكثر وسائل الأمن شيوعاً في بيئة نظم المعلومات :-

■ برمجيات كشف ومقاومة الفيروسات

بالرغم من أن تقنيات مضادات الفيروسات تعد الأكثر انتشاراً وتعد من بين وسائل الأمن المعروفة للعموم، إلا أنها حجم تطبيق هذه التقنيات وإستراتيجيات وخطة التعامل معها تكشف عن ثغرات كبيرة وعن أخطاء في فهم دور هذه المضادات، وبالمعموم ثمة خمسة آليات أساسية لكيفية تحري هذه المضادات للفيروسات التي تصيب النظام، كما ثمة قواعد أساسية تحقق فعالية هذه الوسائل والتي تعتمد في حقيقتها على الموازنة ما بين ضرورات هذه التقنيات لحماية النظام وما قد يؤثره الاستخدام الخاطئ لها على الأداء وفعالية النظام .

• الجدران النارية Firewall والشبكات الافتراضية الخاصة virtual private networks .

تطورت الجدران النارية بشكل متسارع منذ نشأتها حين كانت تقوم بتصفية حركة البيانات اعتماداً على قوانين ومعاملات بسيطة . أما برمجيات الجدران النارية الحديثة، ورغم أنها لا تزال تقوم باستخدام أسلوب فلترة وتصفية البيانات الواردة، فإنها تقوم بعمل ما هو أكثر بكثير مثل إنشاء الشبكات الافتراضية الخاصة virtual private networks ، رقابة محتوى البيانات الوقاية من الفيروسات، وحتى إدارة نوعية الخدمة quality of service، وهذه الخدمات جميعها تعتمد على ميزة أساسية وهي أن الجدران النارية تقع على طرف الشبكة، والجدران النارية كانت توضع على ما يعرف بالمستشفيات الحصينة Bastion Host وأول جدار ناري من هذا النوع، يستخدم الفلاتر وبوابات التطبيقات (البرمجيات الوسيطة Proxy) كان من شركة ديجيتال كوبيمنت، وكان يعتمد على الجدار الناري من شركة Dec حيث أن مختبرات الشبكات التابعة لشركة Dec هي التي وضعت أول الجدران النارية التي أنتجتها الشركة

من هذه البدايات البسيطة، دفع التنافس الحاد بين المزودين للحصول على حصة سوقية من سوق الجدران النارية، إلى المزيد من الابتكارات، ليس فقط في مجال تسريع أداء الجدران النارية وتقديم خدماتها، بل وأيضاً في تضمينها قدرات متعددة تفوق ما كان متوفراً في تلك الأيام، وتتمثل هذه القدرات بما يلي :-

- التحقق من هوية المستخدمين :- ذلك أن أول ما أضافه المطورون إلى الجدران النارية الأولى كانت القدرات القوية للتحقق من الهوية، وإذا كانت السياسات الأمنية التي تتبعها المؤسسة تسمح بالنفاذ إلى الشبكة من شبكة خارجية، مثل الإنترنت، فإنه لا بد من استخدام ميكانيكية ما للتحقق من هوية المستخدمين . والتحقق من الهوية يعني ببساطة التأكد من صحة هوية المستخدم بشكل يتجاوز مجرد التحقق من اسم المستخدم والكلمات السرية والتي لا تعتبر بحد ذاتها وسيلة قوية للتحقق من هوية المستخدمين . ذلك انه وعلى وصلة غير خاصة، مثل وصلة غير مشفرة عبر الإنترنت، فإن أسماء المستخدمين وكلماتهم السرية يمكن نسخها وإعادة استخدامها Attacks Replay، أما الأساليب القوية للتحقق من هوية المستخدمين فتستخدم أساليب التشفير مثل الشهادات الرقمية Certificates أو برمجيات حساب الشفرات الرقمية الخاصة . وبواسطة الشهادات الرقمية يمكن هجمات إعادة الاستخدام حيث يتم نسخ اسم المستخدم وكلماته السرية وإعادة استخدامها للنفاذ إلى الشبكة .

- الشبكات الافتراضية الخاصة :- أما الإضافة الثانية إلى الجدران النارية للإنترنت فكانت التشفير البيني للجدران النارية firewall - to firewall وكان أول منتج من هذا النوع هو virtual interlock، وهذه المنتجات هي ما ندعوها اليوم بالشبكات الافتراضية الخاصة virtual private networks . وهذه الشبكات خاصة لأنها تستخدم التشفير، وهي افتراضية خاصة لأنها تستخدم الإنترنت وشبكات عامة لنقل المعلومات الخاصة.
- مراقبة المحتوى Content Screening :- أصبح من الشائع استخدام الجدران النارية كأدوات لمراقبة المحتوى الوارد إلى الشبكة .
- ومن بعض الإضافات التي وضعت في برمجيات الجدران النارية هي البحث عن الفيروسات، ومراقبة عناوين الإنترنت، منع برمجيات جافا، وبرمجيات فحص ومراقبة الكلمات السرية.
- الجدران النارية الخاصة firewall appliances :- وهو جيل جديد من الجدران النارية. وهذا الجيل يحتوي على عدد من التقنيات بما في ذلك حلول جدران نارية جاهزة turnkey بمعنى أنها لا تحتاج إلى إصدار من قبل المستخدم ويمكن البدء باستخدامها فور الحصول عليها دون الحاجة إلى إجراء أية تعديلات خاصة على نظام التشغيل أو البنية التحتية المستخدمة .
- التشفير

تغطي تقنيات وسياسات التشفير باهتمام في ميدان أمن المعلومات، ومرد ذلك أن حماية التشفير يمثل الوسيلة الأكثر أهمية لتحقيق وظائف الأمن الثلاثة، السرية والتكاملية وتوفير المعلومات، فالتشفير تقنيات تدخل في مختلف وسائل التقنية المنصبة على تحقيق حماية هذه العناصر، فمسان سرية المعلومات أصبح يعتمد من بين ما يعتمد على تشفير وترميز الملفات والمعطيات بل تشفير وسائل التثبيت وكلمات السر، كما أن وسيلة حماية سلامة المحتوى تقوم على تشفير البيانات المتبادلة والتثبت لدى فك التشفير أن الرسالة الإلكترونية لم تتعرض لأي نوع من التعديل أو التغيير، ويعد التشفير بوجه عام وتطبيقاته الجديدة وفي مقدمتها التوقيعات الإلكترونية، الوسيلة الوحيدة تقريبا لضمان عدم إنكار التصرفات عبر الشبكات الإلكترونية، وبذلك فإن التشفير يمثل الاستراتيجية الشمولية لتحقيق أهداف الأمن من جهة، وهو مكون رئيس لتقنيات ووسائل الأمن الأخرى، خاصة في بيئة الأعمال الإلكترونية والتجارة الإلكترونية والرسائل الإلكترونية وخصوصا البيانات المتبادلة بالوسائط الإلكترونية .

ومن حيث مفهومه، فإن التشفير يمر بمرحلتين رئيسيتين، الأولى تشفير النص على نحو يحوله إلى رموز غير مفهومة أو مقروءة بلغة مفهومة، والثانية، فك الترميز بإعادة النص المشفر إلى وضعه السابق كنص مفهوم ومقروء، وهذه المسألة تقوم بها برمجيات التشفير التي تختلف أنواعها ووظائفها . أما من حيث طرق التشفير، فتمتد التشفير الترميزي، والتشفير المعتمد على مفاتيح التشفير، التي قد تكون مفاتيح عامة أو خاصة أو مزيجا منها، وللوقوف على أبرز أغراض وعناصر التشفير وطرقه التقنية نورد تاليا مواد مختارة تتناول هذه المسائل مع الإشارة إلى مصادرها .

قواعد البيانات القانونية

د. رؤوف هلال

helal_raouf@hotmail.com

2- وظائف بنوك وقواعد المعلومات القانونية :

تدور وظائف قواعد وبنوك المعلومات القانونية في فلك ثلاث وظائف رئيسية هي :

- اقتناء المواد القانونية

- تحليلها

- بثها بواسطة استخدام الحاسب الآلي

3- أنواع بنوك وقواعد المعلومات القانونية :

بنوك وقواعد المعلومات القانونية تندرج تحت بنوك وقواعد المعلومات المتخصصة على أساس أنها تهتم بقناة موضوعية معينة وهى القانون، وتنوع هذه البنوك وقواعد المعلومات إلى : بنوك وقواعد معلومات تجارية، وبنوك وقواعد معلومات غير تجارية.

4- مكونات بنوك وقواعد البيانات القانونية :

- المدخلات Inputs :

وهى مجموعة البيانات والمواد والوثائق الخاضعة للنظام والتي سوف يتناولها . ويعتمد فى توفير هذه المدخلات عادة على مصادر المعلومات وأوعية نقلها المختلفة، والتي تدخل فى نطاق تخصص البنك أو القواعد. وهناك خطوات أساسية وإجراءات فنية لابد من مراعاتها وتنفيذها بغية تأمين هذه المدخلات

(1) اقتناء المعلومات Acquisition

(2) تحليل وتنظيم المعلومات Analyzing

and Organizing

(3) إدخال المعلومات Input

تهدف هذه المقالة إلى التعريف ببنوك وقواعد المعلومات القانونية، مع بيان أهم وظائفها، وأنواعها، ثم مجموعة العناصر المكونة لها، والمستفيدين منها، مع عرض نماذج لأهم بنوك وقواعد المعلومات القانونية فى البلدان الأجنبية. وأيضا بنوك وقواعد المعلومات القانونية فى مصر، بهدف التعرف على أهميتها وطرق استخدامها.

1- التعريفات والتسميات :

ارتبط مفهوم "بنك المعلومات" ارتباطاً وثيقاً باستخدامات الحاسب الآلي، حيث إن ظهور مصطلح " بنك المعلومات " تزامن مع ظهور أجهزة الحاسب الآلي واستخدامها فى تخزين واسترجاع المعلومات. وذلك يعرف بنك المعلومات بأنه " مركز يتعامل مع المعلومات ويوثقها بشكل آلى عن طريق استخدام أجهزة الحاسب الآلي بأشكالها وأنواعها المختلفة "

أما قاعدة المعلومات Database فهى عبارة عن " مجموعة مشتركة من البيانات المهيكلية والتي تديرها رزمة برمجيات خاصة تعرف باسم نظام إدارة قواعد المعلومات، وتستخدم بواسطة عدة برامج تطبيقات " ويحتوى بنك المعلومات عادة على قاعدة للمعلومات، أو مجموعة من قواعد المعلومات للربط بين مداخل بيانات معينة، وهذا ما يفسر استخدام مصطلح " قاعدة المعلومات " كثيراً فى أدبيات الموضوع للدلالة على مفهوم بنك المعلومات "

3. دقة مخرجاتها من المعلومات نتيجة للمراجعة المستمرة والدقيقة على السواد المدخلة.
4. تنوع طرق استرجاع المعلومات.
5. إمكانية استخدام مخرجاتها كبديل عن اقتناء مواد قانونية جديدة.

- المستخدمين Users :

يمثل المستخدمون أحد مقومات عمل مجموعة عناصر بنوك وقواعد المعلومات، فمنهم تستمد هذه البنوك وقواعد المعلومات وجودها، وبهم تتأثر من حيث مدى تحقيق متطلباتهم. ولذلك من المهم تحديد المستخدمين والتعرف على احتياجاتهم من خدمات المعلومات، كذلك ينبغي العمل على تنمية وتشجيع المستخدمين على استخدام المعلومات المتوافرة، وإرشادهم وتوجيههم إلى أسس الطرق للحصول على المعلومات، إلى جانب الاهتمام بمقترحاتهم بشأن تطوير الخدمات التي يقدمها البنك .

5- بنوك وقواعد المعلومات الأجنبية

Foreign Legal Databases and Banks

اتجهت كثير من البلدان الأجنبية في الآونة الأخيرة إلى استخدام أنظمة آلية قانونية، بغرض التغلب على كثير من مشاكل البحث اليدوي في ظل تدفق القرارات والتشريعات والأحكام القانونية، وتسهيل مهمة القضاة والمحامين في تتبع هذا الكم الهائل من المعلومات القانونية، وتخفيفاً لسرعة الفصل في القضايا الجارية، ومن جانب آخر فسيط هذا الكم من القرارات والتشريعات والأحكام الجديدة. والتأكد من عدم تعارضها مع النصوص القانونية القائمة بالفعل.

(4) تخزين ومعالجة المعلومات Storing and Processing

(5) استرجاع المعلومات Information Retrieval

- المعالجة أو العمليات : Processing

ويقصد بها عملية تحويل البيانات والمواد والوثائق إلى معلومات مفيدة، وذلك باستخدام عناصر تكنولوجية معالجة المعلومات .

- المخرجات : Outputs

يقصد بالمخرجات مجموعة المعلومات المطلوب الحصول عليها من النظام لتقديمها إلى المستخدمين، ولذلك تعتبر المخرجات من العناصر الهامة والمؤثرة، التي يتوقف عليها نجاح النظام أو فشله، حيث إنها المبرر الحقيقي عن احتياجات المستخدمين.

وتتنوع مخرجات بنوك المعلومات وتختلف من بنك إلى آخر تبعاً لاختلاف أهدافها : فهناك بنوك وقواعد معلومات تقتصر مخرجاتها على المعلومات البيبليوجرافية، وأخرى تقتصر على المعلومات النصية، وهناك ما تكون مخرجاتها مزيجاً من المعلومات البيبليوجرافية والنصية مما.

وتتأثر مخرجات بنوك وقواعد المعلومات وتتفاوت من بنك إلى آخر - من حيث دقتها وسرعة بثها وتنوع طرق استرجاعها - تبعاً لتفاوت مجموعة العناصر المكونة لها. فأهم ما يميز بنوك وقواعد المعلومات القانونية عن غيرها من أنظمة المعلومات القانونية الأخرى ما يلي :

1. السرعة الهائلة في فحص وفرز المواد مهما كثر عددها.
2. السرعة الهائلة في بحث المعلومات الجديدة مقارنة بطرق البحث التقليدية.

إلى حد كبير مع "LEXIS" في عمق التغطية ودرجة الكفاءة
- مميزات نظام لكسيس:

LEXIS SYSTEM

- (1). برنامج نصي كامل.
- (2). يميز القرارات والتشريعات والأحكام المتشابهة.
- (3). يسهل الحصول على الأحكام التي أصدرها قاضي معين.
- (4). يسهل الحصول على القضايا التي ترفع فيها محامى معين.
- (5). يوفر قوائم هجائية بالمصطلحات القانونية التي وردت في الوثائق المدخلة.
- (6). يحدث يوميا.

- الأنظمة القانونية غير التجارية

Noncommercial Legal Information Systems

تتعدد الأنظمة غير التجارية التي تتبع الجهات الحكومية والجهات العلمية في البلدان الأجنبية ما بين أنظمة يتاح استخدامها على الخط المباشر On-Line وأنظمة متاحة للاستخدام الداخلي فقط On-Line نظرا لسرية المعلومات التي تحتويها

- مميزات نظام JURIS

ففي الولايات المتحدة هناك نظام "JURIS" الذي يتبع وزارة العدل Department of Justice وهو متاح على الخط المباشر. وبعد من أشهر الأنظمة الحكومية يرجع تاريخ العمل به إلى سنة 1970.

- (1). برنامج نصي كامل.
- (2). يعتمد على نظام تشغيل يسمح بإجراء حوار بين المشغل والحاسب.

فلقد شهدت بدايات عام 1980 نمواً وتنوعاً كثيراً من الأنظمة الآلية القانونية - ما بين أنظمة تجارية، وأنظمة غير تجارية - يمكن الاعتماد عليها في البحث، حيث تمتاز بالخبرة والكفاءة وعمق التغطية.

- الأنظمة القانونية التجارية :

Commercial Legal Information

امتازت الولايات المتحدة الأمريكية دون غيرها من الدول، بتعدد الأنظمة الآلية القانونية ولاسيما التجارية. فمن أشهر هذه الأنظمة : نظام "LEXIS" الذي تسوقه شركة "Mead Data Central" ونظام

"WESTLAW" الذي تسوقه شركة "West Publishing Company" ونظام "AUTO -CITE" الذي تسوقه شركة "Lawyers Co-operative Publishing Company."

وفى كندا هناك نظام "QL Systems Ltd." أما فى المملكة المتحدة وبقية بلدان الاتحاد الأوروبي فهناك نظام "EUROLEX" والذي كان يسوقه "European Law Butter Center Ltd." وحاليا يسوقه

Worth

ويعد نظام "LEXIS" الذي يرجع تاريخ نشأته إلى سنة 1973 من أشهر الأنظمة القانونية وأوسعها انتشاراً على المستوى العالمي، وينافسه فى نفس الدرجة فى الوقت الحالي نظام "WESTLAW" الذي كان يقدم خدماته من خلال "LEXIS" ثم انفصل عنه سنة 1982، حيث اكتملت قواعده وأصبح متشابهاً

فوائد ومميزات قواعد وينوك المعلومات المصرية: على الرغم من بعض نقاط الضعف التي تعاني منها وينوك وقواعد المعلومات القانونية في مصر، إلا أنها لها من الفوائد والمميزات، ما يجعلها أداة مهمة وأساسية لا غنى عنها في مجال البحث القانوني، فمن أهم هذه الفوائد والمميزات :
- فوائد ومميزات قواعد وينوك المعلومات المصرية:

1. مراجعة وتطوير التشريعات وتقنينها في مجموعات متخصصة.
 2. دعم اتخاذ القرارات، لاسيما فيما يتعلق بالجهات التشريعية والتنفيذية.
 3. المساهمة في تحقيق الدقة والسرعة في توفير المعلومات اللازمة لرجال القانون.
 4. توفير خدمة سريعة وحديثة للمواطنين، تكفل لهم تحقيق أبسط حقوقهم في الاطلاع على النصوص التشريعية التي تحكم علاقاتهم وتحدد واجباتهم وحقوقهم.
 5. تسهيل مهمة الرقابة القضائية على الأحكام.
 6. ضمان عدم تصادم القوانين والتشريعات.
 7. الوقوف على أحدث التطورات لكل قانون أو تشريع.
 8. وبالإضافة إلى ذلك هناك من الفوائد والمميزات التي يمكن إجمالها فيما يلي : العمل على سرعة التقاضي.
 9. تنمية الإنتاج الفكري في مجال القانون.
 - 10- الاستفادة من مخرجاتها كبديل عن اقتناء بعض المواد القانونية.
- في النهاية يمكن أن نقول إن وينوك وقواعد البيانات القانونية أصبحت أداة أساسية لا غنى عنها لرجل القانون.

(3). يميز القرارات والتشريعات والأحكام المتشابهة.

(4). يميز الأحكام التي أصدرها قاضي معين.

(5). يميز القضايا التي تراعى فيها محامى معين

(6). يوفر قوائم هجائية بالمصطلحات القانونية التي وردت في الوثائق المدخلة.

(7). يحدث بصورة مستمرة.

6- بنوك وقواعد المعلومات القانونية في مصر
النشأة والهدف :

يرجع تاريخ إنشاء بنوك وقواعد المعلومات القانونية في مصر إلى بداية الثمانينيات، ففي عام 1981 أنشئ بنك المعلومات القانونية والقضائية للنشترتي، وهو بنك معلومات تجاري، يهدف إلى ميكنة مجموعة أحكام محكمة النقض المدنية والجنائية، لتسهيل الاستفادة منها والإلمام بها، باعتبارها أداة معاونة، تمكن القضاة في الفصل في القضايا الجارية بسرعة، بشرط وجود نص تشريعي يلزم به القاضي.

وفي عام 1987 أنشئ مركز معلومات ودعم اتخاذ القرار التابع لمجلس الوزراء " القاعدة القومية للتشريعات المصرية "، وذلك بهدف حصر التشريعات والقرارات الصادرة في مصر منذ عام 1824 إلى وقتنا الحاضر، وتحديد العلاقات فيما بينها، بفرض الإصلاح التشريعي في مصر، وعدم تصادم النصوص التشريعية بعضها البعض.

وفي أواخر عام 1989، أنشأت وزارة العدل بنكاً للمعلومات القانونية في محكمة النقض، أطلق عليه اسم " مركز المعلومات القضائي " وذلك بهدف ميكنة مجموعة أحكام محكمة النقض المدنية والجنائية لمنع تضاربها من جهة ولتسهيل الاستفادة منها من جهة أخرى، وهو نفس الهدف تقريبا الذي أنشئ من أجله " بنك المعلومات القانونية والقضائية للنشترتي."

المبادئ الكبرى للحكومة الإلكترونية

د. عمر محمد بن يونس

مقدمة:

الحكومة الإلكترونية منهي عمل تقني - إنساني يؤدي خدمات جليلة للفرد في كافة مجالات الحياة التي يمكن أن تتصل بتكنولوجيا المعلومات. لذلك يرتبط فهم القيم الصحيحة للحكومة الإلكترونية بمدى ما يمكن أن تقدمه للإنسان الفرد في كل مكان. وأكثر ما تلتزم به الحكومة الإلكترونية كمنهج هو ارتباطها بهدم سلبيات العمل الإداري وبذلك فهي تضع الفلسفة الفردية الاجتماعية في صيغة جديدة قابلة للنقاش والجدل وإحياء معالم الإنسانية المهددة التي كانت محلا لوعود واهتمام كافة المواثيق الدولية والمحلية. فالفرد حول العالم في الفترة المعاصرة يتلقى خدمات متتالية تعبر عن مدى الفوارق الكيفية والكمية بين الأمم. وهو بحاجة إلى قيمة الشائعة التي فقدتها أثناء مرحلة الاندماج في عقيدة الدولة التي وصلت معالمها في بعض الدول إلى إهدار تلك القيم.

وفي هذه الورقة سوف نعرض للمبادئ الكبرى للحكومة الإلكترونية. وسوف نتطرق إلى هذا الموضوع في صيغة ورقة عمل وصولا إلى العرض العام الأولى لتلك المبادئ مستهدفا بذلك طرح الفكرة لفقه القانون والسياسة وعلم الاجتماع... الخ. فإرساء مبادئ كبرى للحكومة الإلكترونية يعني في الحقيقة أن هذه المبادئ يمكن أن تجد لها

موضعا في الدستور الرن أو الجامد. وفي كل الأحوال يجدر الإشارة إلى أن المبادئ الكبرى للحكومة الإلكترونية من طبيعة جامدة لا يمكن اعتبارها مرنة وذلك استنادا إلى مصدرها النابع من التقنية، فلم تكشف عنها الحوادث التاريخية أو المواقف الإنسانية وإنما الذي صنع مقدماتها الأولى أفكار تطبيقية لتكنولوجيا المعلومات.

وإذا كانت الكلمات السالفة تغطي عليها النواح المباشرة فإنه يمكن إعادة صياغة قانونية لهذه الكلمات من حيث طرح المفهوم التقني الإنساني للحكومة الإلكترونية في شكل ضرورة المطالبة بتطبيق مفاهيم الحكومة الإلكترونية في صيغة تعمل على إعادة إحياء المفاهيم الضرورية والإنسانية للفرد. فالفرد اليوم يستطيع إنهاء أعماله الإدارية دون أن يكون عرصة للمضايقة الوظيفية أو التمسف في استعمال أو استخدام السلطة وبما يستتبع ذلك القول بإمكانية هذا الفرد إنهاء كافة أموره الإدارية وفق مبدأ المشروعية وذلك باستخدام منهجية الحكومة الإلكترونية.

والآن نأتي إلى التساؤل مضمون هذه الورقة: ما هي تلك المبادئ الكبرى للحكومة الإلكترونية؟ هناك أربعة مبادئ يمكن أن تكون نواة حقيقية يتشكل على ضوئها الأسس الكبرى للحكومة الإلكترونية:

Electronic Government Act² of الذي يسعى إلى إيجاد هذه المنطقة (اللا

² Public Law 107-347, December 17, 2002 (HR 2458), See: <http://www.access.gpo.gov> مع الأسد في الاختيار أن أول مشروع قانون الحكومة الإلكترونية في الولايات المتحدة الأمريكية كان قد تقدم به عضو مجلس الشيوخ الأمريكي Joseph Lieberman إلى المجلس US Senate 101 / 5 / 1 (S.803). ونفس صرح الرئيس الأمريكي بوش الابن عشية صدور القانون في 12 / 17 / 2002 نال:

Today I have signed into law H.R. 2458, the "E-Government Act of 2002." This legislation builds upon my Administration's expanding E-Government initiative by ensuring strong leadership of the information technology activities of Federal agencies, a comprehensive framework for information security standards and programs, and uniform safeguards to protect the confidentiality of information provided by the public for statistical purposes. The Act will also assist in expanding the use of the Internet and computer resources in order to deliver Government services, consistent with the reform principles I outlined on July 10, 2002, for a citizen-centered, results-oriented, and market-based Government. Title II of this Act authorizes agencies to award "share-in-savings" contracts under which contractors share in the savings achieved by agencies through the provision of technologies that improve or accelerate their work. The executive branch shall ensure, consistent with applicable law, that these contracts are operated according to sound fiscal policy and limit authorized waivers for funding of potential termination costs to appropriate circumstances, so as to minimize the financial risk to the Government.

Title III of this Act is the Federal Information Security Management Act of 2002. It is very similar to title X of the Homeland Security Act of 2002, which also bears the name Federal Information Security Management Act of 2002 and which I signed into law on November 25, 2002. I am signing into law the E-Government Act after the enactment of the Homeland Security Act, and there is no indication that the Congress intended the E-Government Act to provide interim provisions that would apply only until the Homeland Security Act took effect. Thus, notwithstanding the delayed effective dates applicable to the Homeland Security Act, the executive branch will construe the E-Government Act as permanently superseding the Homeland

1. مكافحة الانتقائية في العمل الإداري.
2. إزالة الحواجز (مجتمع معلوماتي واحد).
3. المنهجية الفردية وتطوير القدرات.
4. خلق بيئة حرة فكريا (حرية تجول المعلومة والكشف عن مناطق التفكير والرأي والتعبير).

أولا : مكافحة الانتقائية في العمل الإداري:

من الأهمية بمكان ملاحظة الدلالات العميقة التي تشير إلى الحكومة الإلكترونية كمصطلح يمكن أن يحقق نجاحا كبيرا في مكافحة عدم انتظام الإدارة ماديا من خلال تنظيمها عبر العالم الافتراضي عموما والإنترنت على وجه الخصوص، فيما يعرف بمصطلح .. "ميكنة

L'Administration¹ الإدارية

Electronique. فهذا المصطلح يفيد أن

قدرا من الحرية المتعارف عليها يمكن أن يمارس في المجتمع المعلوماتي دون أية قيود ما دام هناك تنظيمها يعترف به القانون يشكل منطقا وميارا لهذه القيود. ولكي تصبح فكرة الحكومة الإلكترونية ناجحة في المجتمع المعلوماتي يجب

أن يكون هناك منطقة "لا سياسية خالصة Non

"Political Zone" تعمل من خلالها هذه

الحكومة، فضلا عن الاهتمام بالمهام الإدارية في

عمل الحكومة هذا. ونجد لهذه المنطقة تطبيقاتا في

قانون الحكومة الإلكترونية الفيدرالي الأمريكي

المؤرخ 17 ديسمبر 2002 The

¹ محمد بن يونس - مستشفيات ومتفرقات - مقدمة الإصدار المباشر لموسوعة التشريعات العربية 2000. - انظر كذلك مؤلفنا المصنف الممارسات والحكومة الإلكترونية - الطبعة الثانية - طر الهيئة العربية القاهرة: 2005 ص. 204 وما بعدها.

فتتبرز هذه القيود من خلال الالتزام بالنظام بداية. ومثل هذا الالتزام يخلق معيارية تتكامل مع الفكر الإنساني، فلا تضيء الإجراءات قدما ما دام هناك خلا في الالتزام المشار إليه. فمثلا من يتوجه إلى احد المواقع بقصد استخراج بطاقة شخصية أو جواز سفر يلزمه هنا ملء النماذج بالكامل، فإذا ترك فراغ في احد البيانات فإن ذلك يترتب عليه عدم إمكانية استخراج هذه البطاقة أو غيرها من المستندات التي تيسر حياة الإنسان. فإذا تقدمنا خطوة إلى الأمام فإن ترك فراغات في المثال السالف سوف يمنع الرقم القومي لهذا الشخص من الوجود، كل ذلك محسوباً على الدقة المتناهية التي يكون عليها اتصال الأفراد بالحكومة الإلكترونية.

وتبدو الحكومة الإلكترونية أكثر حدة على العقل البشري في الزمن المعاصر إذا حاولنا استخدام الإمكانات الكاملة لتكنولوجيا المعلومات لتحقيقها، ففي هذه الحالة سوف يكون هناك تجاوزاً لما هو مقرر حول الحكومة الإلكترونية فيبدو الأمر كما لو كان الإنسان يتناول الخيال! وسوف تقابل الإمكانات الكاملة لتكنولوجيا المعلومات بالرفض أيضاً، وذلك نظراً لعدم وجود هامش اشتغالي فيها على الإطلاق من الناحية الإدارية والمالية.

ثانياً: إزالة الحواجز (مجتمع معلوماتي واحد):

ماذا يعني مصطلح " إزالة الحواجز " ؟

إن استخدام هذا المصطلح يميز عن القيمة الحقيقية للمجتمع المعلوماتي ، إلا أن هذه القيمة تتخذ في الشكل المادي لها صيغة مثالية ، ويبرز ذلك في

سياسية الخالصة في مجال العمل الإداري والمالي وبما يترتب على ذلك انتفاء حركة الانتقائية بالكامل، وهي الحركة التي تجعل مبدأ المساواة بين البشر متخلفاً عن الوجود، ولقد كانت مسألة الانتقائية هذه محض إزعاج للدورة الرابعة والخمسين للجمعية العامة للأمم المتحدة³ ، حيث اعترفت بكونها نقيض المساواة والحياد والموضوعية فتم اعتبار وجود الانتقائية أمر يتعارض مع حقوق الإنسان .

فإذا تقلصت الانتقائية فإن المعاملات الإنسانية سوف تتشعب من وراء الحكومة الإلكترونية فتتخذ بالضرورة الشكل المثالي، فكلما كان مصطلح الحكومة الإلكترونية مستوجداً كلما كانت الصلاحيات الممنوحة لعضو الإنترنت مقيدة بسلسلة طويلة من القيود النفسية والموضوعية،

Security Act in those instances where both Acts prescribe different amendments to the same provisions of the United States Code.

Finally, the executive branch shall construe and implement the Act in a manner consistent with the President's constitutional authorities to supervise the unitary executive branch and to protect sensitive national security, law enforcement, and foreign relations information. In particular, consistent with my constitutional authorities and section 301(c) of this Act, the executive branch shall construe the Act in a manner that preserves the authorities of the Secretary of Defense, the Director of Central Intelligence, and other agency heads with regard to the operation, control, and management of national security systems.

GEORGE W. BUSH, THE WHITE HOUSE, December 17, 2002.

³ قرار الجمعية العامة للأمم المتحدة رقم 54 / 174 المؤرخ 15 / 12 / 2000

بشأن تمرير إجراءات الأمم المتحدة في مجال حقوق الإنسان بحسب القانون الدولي وأهمية العلاقات والمبادئ والموضوعية - الدورة 54 - البند 116 (ب) - من جدول الأعمال . وقررها رقم 56 / 153 المؤرخ 19 / 12 / 2001 - الدورة 56 ، وقررها رقم 57 / 203 المؤرخ 18 / 12 / 2002 - الدورة 57 . كذلك انظر موقف ليبيا من الانتقائية منشوراً في الملاحق.

الافتراضي (ملحق المعاهدة الأوربية حول الجريمة في العالم الافتراضي).
 فإذا قبلنا وجود تفريد بشري في العالم المادي في علاقة الإنسان بالحواجز، فإنه لا يمكن تصوير المجتمع المعلوماتي على أنه يتكون من مجموعة من المجتمعات متعددة المشارب والاتجاهات كما هو الحال في المجتمع المادي، فهو مجتمع واحد فقط، وبحيث يمكن مناظرته بمجتمع آخر له وجود في الفكر المثالي في العالم المادي وهو "المجتمع الإنساني".

ولا يعني ذلك عدم وجود خلاف في المجتمع المعلوماتي وإنما لن يكون سند الخلاف سندا سياسيا مبنيا على قواعد الحدود والحواجز التي تقيمها الدول انطلاقا من مفاهيم سياسية.
 فالخلاف يبنى في المجتمع المعلوماتي على أسس الحضارة والانتماء العائلي الذي يجب أن يجد له محلا في تبادل الفكر والتنوع الثقافي والنشاط الذهني وحركة التاريخ.. الخ، دون أن يكون أساسه نقل الخلافات المتواجدة في العالم المادي إلى هناك، ودون أن يكون الأمر متعلقا ببناء سياسي له جذور مادية مثلا في الدولة. ومثل هذا الأمر انتهت إليه الأمم المتحدة بنوع من الحذر، لذلك لم تمنح الجمعية العامة للأمم المتحدة في عام 1999 من طرح فكرة "الحوار بين الحضارات" بوسائل من بينها نشر المعلومات وتنظيم الحلقات الدراسية وتنظيم المؤتمرات.. الخ⁴ وهذه الوسائل

حركة عاطفية تهدف إلى الترويج للإنترنت كصيغة إعلانية صحفية وإعلامية. ولا ماذا يعني وجود عوائق في العالم المادي تجعل مصطلح إزالة الحواجز قائما في العالم الافتراضي؟
 والحقيقة أن مصطلح "إزالة الحواجز" يتخذ بعدا جديدا في التفسير يشير إلى إمكانية الحصول على المعلومة في المجتمع المعلوماتي طالما وجد لها مكانا في العالم الافتراضي، بمعنى أنه قد تم وضعها هناك. ولا يعني مثل هذا المصطلح إزالة الحدود السياسية مثلا بين الدول، فمثل هذه الحدود ليست فرضا سياديا أمام كافة البشر، بل أن هناك تقسيمات سياسية تعتمد مبدأ حيازة جواز السفر يمكنها أن تزيل حاجز الحدود أمام شخص دون آخر، فمن يملك جواز سفر يوناني مثلا يستطيع الدخول إلى فرنسا أو بريطانيا ولا توجد حواجز من أي نوع لديه في حين يحتاج جواز السفر العربي إلى ما يفيد إزالة هذا الحاجز الموضوع أمامه/ التأشيرة.

فالحواجز موجودة في العالم المادي وبما يوحي وجودها وكيونيتها هنا بوجود وكيونيتها تفريد في الجنسية والمواطنة وجوازات السفر.. الخ، وبما يوحي بالسند السياسي لهذا التفريد البشري وجود نوع من إقامة الحواجز العرقية والتعريفية عموما. ومثل هذه الإجراءات المتخذة ضد بعض البشر يمكن استخدام الأدوات القضائية لردعها، وليس هناك ما يمنع من تطوير آليات المعاهدات والاتفاقيات الدولية في هذا الإطار في مسمى التمييز والتمييز والعرق والجنس واللون والدين في مواجهة الحواجز المشار إليها كما هو الحال في اتجاهات التشريع الدولي فيما يتعلق بالعالم

⁴ قرار الجمعية العامة للأمم المتحدة رقم 113 / 45 للورخ 12 / 7
 2000 بشأن سنة الأمم المتحدة للحوار بين الحضارات، الدورة
 54، البند 34 من جدول الأعمال.

ثالثا: المنهجية الفردية وتطوير القدرات:

لكي يتم إعداد حلقة متكاملة من التواصل الإنساني في العالم الافتراضي يلزم، فضلا عن الاعتراف بوجود المجتمع المعلوماتي والحكومة الإلكترونية، وجود صيغة أو تفسير لمصطلح الفردية. ذلك أن الفرد في العالم الافتراضي يتسع لأكثر من مجرد ذلك الذي تعترف به الدولة في سجلاتها، سواء كان من مواطنيها أو من المقيمين بها. فالفرد في المجتمع المعلوماتي يمكن أن يكون آليا دون تردد، ويعترف المجتمع المعلوماتي بهذه النوعية الجديدة من الأفراد وبما يسمح هنا بإحداث التواصل بين الفرد وبين الآلة وبشكل يطمح على المفهوم التقليدي للآلية.

وبناء عليه لا يحتاج التواصل المعلوماتي إلى مجموعة أفراد مرتبطين بجنسية معينة حتى ولو كانت هذه المجموعة عبارة عن مجموعة أشقاء في منزل واحد كل أمام حاسوبه الخاص، فالجنسية معيار يفشل في المجتمع المعلوماتي بالضرورة، سيما مع توجهات مكافحة التمييز العنصري في العالم الافتراضي، كما هو الشأن فيما اتفقت عليه الدول الأوروبية مع اتفاقية مكافحة الجريمة في العالم الافتراضي الموقعة في بودابست 2001، حيث قررت، كما أشرنا سابقا، وجوب الأخذ في الاعتبار مكافحة التمييز العنصري في ملحق خاص بالاتفاقية المذكورة، وقد سبق بعض الدول الأوروبية إلى القيام بنبذ توجه الجنسية في العالم الافتراضي ووصل الأمر بالقضاء البلجيكي إلى إدانة البعض بارتكاب جرائم عنصرية حال التحرش فيما يتعلق بالجنسية أو بالدين أو بالرق .. الخ،

يمكن القيام بها في المجتمع المعلوماتي بكل سهولة.

ويقود هذا المنطق إلى ربط عملية إزالة الحواجز بمصطلح آخر يلزم أن يكون هو التفسير الوحيد له، ونعني به " التدفق المعلوماتي " في العالم الافتراضي، والتدفق المعلوماتي يعني صيرورة المعلومة في حالة تواصل مستمر مع المجتمع المعلوماتي لأنها هي الركن الأساسي فيه. وكلما زادت حركة التدفق المعلوماتي كلما كان هناك انسيابية وسهولة في التعامل مع العالم الافتراضي عموما، وتستمر بالتالي حركة التطوير في تكنولوجيا المعلومات. فإذا توقف هذا التدفق المعلوماتي فإن العالم الافتراضي يقف عند حدود ما تم تحميله عليه، ومع مرور بعض الوقت ينتهي كل وجود لهذا العالم، وبما يعني في النهاية اقتصاره على القيود التي تفرض عليه. وربما ينطبق عليه مثال مكتبة لم يتم تزويدها بالجديد واقتصرت على الموجود فيها وبما يعني في النهاية أن دورها سوف ينحصر في كونها تمثل نسبيا مرحلة زمنية معينة من الحركة الثقافية.

وهنا نستطيع تخيل فكرة التدفق المعلوماتي على أنها تنتمي إلى مبدأ الحق في المعرفة، وهو مبدأ تعرفه الحضارة الإسلامية بشكل فائق. فالأمر يبدو هنا كما لو كان هناك إعادة كتابة التاريخ بشكل أكثر شمولية، لأن ترتبط الوقائع التاريخية بالمؤشرات السياسية ذات الرؤيا الضيقة وإنما بعدى النتيجة التي يمكن أن تحققها معلومة ما.

لا يمكن التواصل معه إلا في ضوء المنهج المعلوماتي. فهي فكرة جديدة أو أن تفسير مصطلح الفردية يحتاج إلى أدوات تفسير جديدة وبشكل يمكن من القول بأن تطوير القائم الآن لا يكفي وحده لسد فهم هذا المصطلح في المجتمع المعلوماتي. فنظام الشبكات **Networks**

الحالي والمستقبلي أيضا لا يمكن أن يتلق مع نموذج الديمقراطية التقليدية من الناحية المعلوماتية ولكنه يتفق مع فلسفة الديمقراطية المباشرة، في حين أن الديمقراطية الغربية التقليدية وجدت ذاتها رقما ملزمة بتحريك الدورة التقنية إلى منتهاها كاللزام علمي تقني يقع على عاتقها. وهنا فإن صدام سوف يحدث بين المنهج النظري المعائدي في الفلسفة الغربية وبين المنهج العلمي لها في معنى جديد لفكرة الصدام الواقع في ذات الهيكلية التي يقوم عليها النظام السياسي في تلك الفلسفة، فهو هنا صدام ذاتي تحديدا لن يكون له وجود في فلسفة الديمقراطية المباشرة على الإطلاق وإنما مركزه الفكر التقليدي فقط.

إن خطوة إلى الأمام في فهم الفردية في المجتمع المعلوماتي تستدعي من الباحث ضرورة البحث عن نقطة البداية هنا، إذ كيف يمكننا التوصل إلى صيغة تمكنا من الحصول على تفسير لمصطلح الفردية؟

نقطة البداية تكمن في حركة الاتصال بالمجتمع المعلوماتي، فهذا المجتمع يبدأ عندما يتصل فرد بعينه بالآلة لكي تمهد له الوصول إلى العالم الافتراضي. وهنا يصبح لدينا فردية افتراضية أو فيما يصطلح على تسميته بـ .. "عضو الإنترنت"

وهو الأمر الذي يوحي بأن اليوم الذي يتم فيه الاستناد إلى أحكام القضاء لأجل الحصول على تأشيرة دخول إلى دول ترفض منح هذه التأشيرة سوف يصبح ممكنا في ظل مفاهيم تكنولوجيا المعلومات وما سوف تحدثه من تأثير في القيم الاجتماعية.

إن تحتاج الفردية إلى صيغة تفسير جديدة يمكن على شونها تحديد الفرد في المجتمع المعلوماتي وبشكل يسمح ببعض المرونة في تقبل الفكرة التقنية، وبحيث تضاف الآلية في تكنولوجيا المعلومات إلى كل تفسير لمصطلح الفرد. وهذا يقودنا بالضرورة إلى نبذ فكرة الفردية التقليدية التي تقوم على نهج الفكر الخاص الذي يروج له أنصار النظرية الاقتصادية / الرأسمالية تحديدا كما هو الشأن في إمكانية استعمال الإنترنت لموضوع الانتخابات في الدول التقليدية مثلا⁵. فهذه النظرية الاقتصادية السالفة تتنازعها رياح التغيير منذ ما يقارب النصف قرن حتى الآن، وبما يدعو إلى التأكيد على أن نموذج الديمقراطية الغربية أصبح تقليديا في معنى إمكانية وجود نماذج أخرى للعملية الديمقراطية لا تتخذ النموذج الغربي قدوة أو مثلا يُحتذى، وبما يمكن عدادها متميزة عن المنهج الغربي المذكور في معنى وجود فكر وأرضية لها تتمتع بخصائص مستقلة.

أما الفكرة الفردية في ضوء التفسير المعلوماتي فمنبتها العالم الافتراضي الذي خلقت الآلة والذي

القاهرة 24 - 27 يناير 2000 - إعلان
 القاهرة : التعليم للجميع في البلدان العربية :
 تجديد الالتزام) فقد أكد إعلان القاهرة على عبارة
 ذات مغزى، بل وذات بعد يعبر عن الظاهرة
 الثقافية المعاصرة في الوطن العربي وبما يشكل
 بحثه لأزمة خطيرة ، ففي صدر الفقرة 33 من
 إعلان القاهرة جاءت عبارة (الوقت يمر ..) ..
 وهذه عبارة ربما يفهمها البعض وربما لا يفهمها
 البعض الآخر ولكن في النهاية فإن المحصلة من
 هذه العبارة أن المسؤولية كبيرة فيما يبدو.
 وهنا يأتي التفسير الجديد للقيم المعلوماتية
 والرقمية في الحركة الثقافية الفردية للإنسان،
 ومثل هذا التفسير يتناقض مع التوجه الفردي في
 الفكر النخبوي القائم، فالمجتمع المعلوماتي له
 ثقافته الخاصة به، والتي يمكن أن يحدث تعارض
 أو تلاق بينها وبين ثقافة المجتمع المادي أو العالم
 التقليدي ولكن لا يمكن أن ينتقل المفهوم التقليدي
 للثقافة الإنسانية برسته إلى المجتمع المعلوماتي.
 وسبب ذلك أن المفهوم التقليدي للثقافة الإنسانية
 له مشاكله ومشكلاته في حين أن المجتمع
 المعلوماتي مبني على أساس عداة ليس مناطق
 خلاف متعددة على الإطلاق وإنما هو منطقة واحدة
 وهي منطقة اتفاق بالضرورة. ومثل هذا الأمر يقود
 في النهاية إلى أنه لا يمكن أن تشكل ثقافة
 المجتمع المعلوماتي جزءاً من ثقافة احد مجتمعات
 العالم المادي، فلا يصح مثلاً القول بأن ثقافة
 المجتمع المعلوماتي هي جزء من تكوين المواطن
 الأمريكي أو الكندي أو الياباني أو الإيطالي أو
 الصيني أو المصري أو .. الخ ، وهو الإحياء الذي

الذي يصبح كذلك بمجرد ولوجه إلى العالم
 الافتراضي مستخدماً الحاسوب على أية شاكلة
 يكون عليها هذا الحاسوب. ف .. عضو الإنترنت
 هنا ليس له جنسية محددة يتعامل بها في
 المجتمع المعلوماتي وإنما له بصمته الخاصة به
 يستخدمها في صيغة عالمية عابرة للحدود التي
 تعترف بالجنسية والمواطنة .. الخ.
 ولما كانت عضوية المجتمع المعلوماتي هنا قد
 دخلت في طور الفكر الشعبي وأصبحت العامة
 تستخدمها كجزء من تكوينها الاجتماعي
 والاقتصادي فإن الحركة التطويرية في التاريخ
 الإنساني سوف تخلق انتقائية إذا تخلف الركب
 عن التحول إلى القيم المعلوماتية. وسوف تلحق
 الانتقائية الأفراد دون مسؤولية تقع على كاهل
 الدول، فما دامت الإنترنت قد انتقلت إلى المرحلة
 الأهلية أو الشعبية فإن الفرد مسؤول عن نفسه هنا
 وبالتالي سوف يتم وصمه بالجهل أو الأمية إذا لم
 يكن أحد أعضاء المجتمع المعلوماتي. لذلك أن
 النتائج التي انتهى إليها المجتمع الدولي فيما
 يتعلق بتنمية الحركة التعليمية في العالم وفق إعلان
 دكا (المنتدى العالمي للتربية في دكا / السنغال
 26 28 إبريل 2000) بـشعار التعليم
 للجميع **Education for all** والذي يعد
 امتداداً لما اعتمدته الإعلان العالمي حول التربية
 للجميع (جومتين / تايلاند 1990) من حيث
 الالتزام الجماعي بالعملية التعليمية يكاد يتخلف
 عن إطار العمل العربي من أجل تأمين حاجات
 التعليم الأساسية في الأعوام 2000 - 2010
 (المؤتمر العربي الإقليمي حول التعليم للجميع -

(المعلوماتية كمنهج) لكون العامل الحضاري الغربي في الفلسفة الإنسانية يقتصر على مفهوم تصدير المعلومة من خلال قنوات محددة بدقة كبيرة، وهي قنوات ظاهرها حقيقي إلا أنها في موقعها المعلوماتي، وعلى الصورة التي يجب أن تكون عليها، توصم بأنها قناة واحدة فقط. وبعد الجهاز الإعلاني أو الإعلامي المالي النسق الذي يسيطر على تنظيم المعلومة في تواصلها مع البشر، فحادثة وواقعة ما لا يمكن تواصل حدوثها مع البشر أو الفرد بدون الجهاز الإعلامي المالي المذكور، على استثناء يتعلق بالرؤيا المباشرة للحدث، وهي رؤيا بالعين المجردة تقتصر على ثلثة من البشر ممن حضروا الحدث، ولا يحدث مثل هذا الاستثناء كثيرا. وفيما عدا ذلك فإن المنطق السمعى - المرنى يمكن أن يكون قاصرا في بلوغ الغاية المطلوبة للمعلومة في تواصلها مع البشر.

وهنا تدخل المعلومة في مرحلة جدل لا ينتهي، سواء من حيث صحتها (تكوين المعلومة) أو من حيث هيبتها أو مصداقيتها (ملكية المعلومة).

لقد ترتب على عدم انتظام مصداقية المعلومة في المجتمع المادي أن استخدم القراصنة البنية الافتراضية كجمال استغلال العدوان على الملكية الفكرية للبيئات ذات المصداقية المعلوماتية الكاملة، مستغلين صعوبات الإثبات وليس استحالة - في هذا الإطار. فقد استخدم التشهير العدوان على حقوق المؤلف بذات الضراوة التي استخدم فيها أنصار القوة المجردة أسلحة التدمير الشامل في ارتكاب العدوان على دول وشعوب مختلفة في المرحلة المعاصرة. والغريب رفض القضاء في بعض الدول الاعتراف بقصور الخبرة الوطنية

جاء به مدلول نتائج قمة مجموعة الثمانية في KANANASKIS في كندا 2002 بشأن أفريقيا والذي يوحي بوجود حركة تصدير ونقل للتكنولوجيا المتخلفة من جديد كذلك التي تم تنفيذها في التسعينيات من القرن العشرين. إذ يجب أن يرتبط المفهوم الثقافي للمجتمع المعلوماتي بالفردية هنا، بحيث يمكن القول أن هذا الفرد (دون اعتبار لجنسيته) هو أحد أعضاء المجتمع المعلوماتي في حين أن الآخر ليس كذلك.

رابعا: خلق بيئة حرة فكريا (حرية تجول المعلومة والكشف عن مناطق التفكير والرأي والتعبير)

إن المعلومات هي مقياس بشري بالضرورة، وحتى الآن فإن تعريف، وبالتالي تحديد، المعلومة يمكن أن يكون مجال علم جديد هو علم المعلومات كمصطلح دخل قاموس العالمي بجدارة فائقة في المرحلة المعاصرة.

إن الأساس الذي تبني عليه حركة المعلومة في الثقافة والفهم الإنساني لا ينطلق في مرحلة العصر الصناعي من نقطة تعريف المعلومة تحديدا وإنما ينطلق من فكر وفلسفة البحث في كيفية اكتسابها من ناحية ثم في البحث في منطق توريدها مرة أخرى، فهذا الأساس يعتمد على السيطرة في حركة توريد المعلومة مع إفساح المجال الكامل لعملية تصديرها. ومثل هذا الأمر لا يمكنه أن يتوافق مع منهج الفكر المعلوماتي في هذا العصر.

ولقد جعل تفسير العصر الصناعي لمصطلح المعلوماتية الجميع في نقطة بداية بعبدة عن المفهوم الذي يطرحه المصطلح في صيغته الجديدة

سدس سكان العالم نابعة من المجتمع المعلوماتي في صيغة جدلية جديدة يطلقها عضو المجتمع المعلوماتي بكثير من التفكير والتحليل وبشكل يتفاعل مع الحدث ذاته، فقد أصبحت تقارير البنك الدولي وتصريحات البيت الأبيض الأمريكي اليومية سهلة المزال في الوقت الذي يتابع فيه سدس سكان العالم أخبار باقي العالم في دقائق بسيطة باستخدام وسيلة الاشتراك في قوائم المراسلات البريدية عبر الإنترنت .

ومن الأهمية بمكان الإشارة إلى ضعف الموقف الإعلامي إزاء العالم الافتراضي، فلم تعد الدول التي تسيطر على الأعلام الدولي قادرة على التحكم في مسار الفكر العربي وقرارة التاريخ، فمن يلجأ إلى المجتمع المعلوماتي / العالم الافتراضي لا يحتاج إلى وسائل الأعلام التقليدية لكي يفهم المعرفة حقها، بل انه لا يلجأ إلى مواقع وسائل الأعلام التقليدية المذكورة إلا للارتباط وفيما هذا ذلك فانه يصل إلى موقع الحدث ذاته ، الذي تنتقله وسائل الأعلام ، لكي يطلع عليه مباشرة، أو مسجلا. وهذا يحتاج إلى تواصل في القيمة المعلوماتية بين الحدث وبين العالم الافتراضي، وهو تواصل لا يحتاج إلى إذن من أية جهة بقدر ما يحتاج إلى مبادرة توصيل المعلومة أو الحدث إلى العالم الافتراضي. وهذا النوع من المبادرات يلزمه التفاعل مع الأحداث، حيث أن العالم الافتراضي يحتاج إلى التواصل الفوري مع الأحداث وبشكل يكون فيه الزمن الافتراضي متفاعلا مع العالم المادي في صورة تقل ما هو حادث إلى العالم الافتراضي. ومن ثم يمكن القول بان شخصا ما يمكنه وضع كاميرا رقمية في حجم القذاحة في

لديه في هذا المجال في الوقت الذي تعدلت فيه التشريعات الوطنية دافعا عن حقوق المؤلف دون الأخذ في الاعتبار خطورة هذا الاتجاه، وان كان في دول أخرى أفسح المجال للخبرة الدولية لتتخذ دورها في هذا الإطار دون حرج أو كلل أو ملل⁶.

وفي النهاية فإن مجتمعا بشريا قابيع في نطاق الإعلام أو الإعلان المادي المقيد لا يستطيع بناء جسور ثقة بهنه وبين أية معلومة تصل إليه تكون عوامل التحليل مفقودة عنده، من حيث عدم ثقته في وسائل أو وسيلة الأعلام العالمية المتصصة بالتوحيدية التي تسيطر على مسار وصياغة المعلومة في تواصلها مع البشر. والثال التطبيقي على ما سلف يجز لنا حال البحث في قنوات صياغة المعلومة في العالم المادي بقصد تواصلها مع البشر، فمثل هذه القنوات على ضخامتها لا تشكل قيمة مساحية أو حيز ما يذكر في المجتمع المعلوماتي، فهي مجرد مواقع أو ورش عمل هناك ، ويحدث يمكن أن يكون موقعا فرديا خاصا بشخص واحد له تأثير اعلامي أقوى منها هناك.

فإذا تحولنا إلى الواقعية فإن سدس عالمنا المعاصر في افتراض نمسي مضمونه عدم وجود عوالم أخرى يمكن أن يكونوا بعيدين اليوم عن المعلومة المصافة ماديا لكونهم يتواصلون مع معلومة أكثر جدية هي المعلومة الرقمية، فهؤلاء وصلوا إلى مرحلة استحداث الجدل العقلي بالضرورة ويبقى عليهم هنا أن تبدأ نقطة انطلاق حقيقية في قياس الجدل العقلي حول المعلومة المصافة في المجتمع المعلوماتي. ففي هذا الإطار نجد أن المعلومة عند

⁶See: Licra v. Yahoo Fr.

ومن الملاحظات المهمة في إطار ميثاق الاتحاد الإفريقي هو تناوله لمسألة المشاركة الشعبية **Popular Participation** في المجال السياسي (المادة 3/ج) كمصطلح تطويري يمكن أن يكون له امتداد إيجابي عبر المجتمع المعلوماتي. وحتى المرحلة المعاصرة فإن مسألة التمييز بين الرأي وبين التعبير وبين المعلومة من الموضوعات ذات الجدلية العقلية التي لم تأخذ حظها بذات المهارة التي يمكن بها اعتبار كل من الرأي والتعبير من مصادر المعلومة⁹. ومثل هذا يؤدي إلى الخلط، وهو ما يخلق العديد من المغارقات في الآلية التي تعمل بها المعلومة. فمثلاً المعلومة أضحيت سلمة (ولم تعد خدمة) في حين أن كل من الرأي والتعبير ليسا من السلع وإنما من الحقوق التي قد يقابلها التزامات وواجبات، سيما من الناحيتين القانونية والأخلاقية.

منزله بقصد تسجيل الوقائع اليومية فيه، فلا يعد ذلك منه مجرد عملية تجسسية يقوم بها على أهل منزله، بل هي كتابة تاريخ رقمي لمنزله وعائلته تسمح للأجيال الجديدة فيها من الاطلاع على نظام عمل الأسلاف، بل ومن الممكن أن يكون أهل المنزل ممن يخضعون لعملية التسجيل السمعي المرئي على دراية وعلم بهذه الكاميرا والغرض المد لها وهم سعداء بذلك.

ويلزم أن يكون هناك مفارقة واضحة بين كل من الرأي **Opinion** وبين التعبير **Expression** وبين المعلومة **Information**. فمثلاً المادة (19) من الإعلان العالمي لحقوق الإنسان تنص على أنه "لكل فرد الحق في حرية الرأي والتعبير"، في حين كانت المادة (9) من الميثاق الإفريقي لحقوق الإنسان والشعوب تنص على أنه "... لكل فرد الحق في استقباله **Receive المعلومات**"⁷. ولقد انضم هذا الميثاق إلى ميثاق الاتحاد الإفريقي المؤرخ 11 يوليو 2000 في المادة (3/ هـ).

⁷African Charter on Human and Peoples' Rights, EIGHTEENTH ASSEMBLY OF HEADS OF STATE AND GOVERNMENT, JUNE 1981, NAIROBI.

1. Every individual shall have the right to receive information.

express and disseminate his opinions within [u] Charter on Human and Peoples' Rights, adopted June 27, 1981, OAU Doc. CAB/LBG/67/3 rev. 5, 21 I.L.M. 58 (1982), entered into force Oct. 21, 1986; [excerpts] ...

Togo, this 11th day of July, 2000. Article 3: Objectives: The objectives of the Union shall be to: h - Promote and protect human and peoples' rights in accordance with the

African Charter on Human and Peoples' Rights and other relevant human rights instruments;

⁹Thomas Cochrane, Note, The law of nations in cyberspace: fashioning a cause of action for the suppression of human rights reports on the internet 4 Mich. Telecomm. Tech. L. Rev. 157 (1998) available at <http://www.mtltr.org/volfour/cochrane.pdf> P. 174

معضلات البحث في اللغة العربية

أ.د. محمد علي سلامة

كلية الآداب جامعة حلوان

نبيهل السيد ورافت الكمار: "يقوم الحاسوب بقص الزوائد واللواحق للكلمة وإعادتها إلى أصلها مجردة من زوائد ولواحقها وردها إلى جذرها الأصلي، وبالتالي يتم اختصار مئات الآلاف من الكلمات في كلمة واحدة هي الجذر"⁽¹⁾.

ولا شك أن هذا مفيد للباحث في اللغة العربية؛ لأن هذا سيفتحه عن العودة إلى المعاجم الثقيلة المطبوعة، ولكن هل راعت هذه المحاولات استقصاء ما جاء في المعاجم العربية كلها؟ ثم هل راعت الكلمات الحديثة الناتجة عن تكنولوجيا العصر الحديث؟ بمعنى أن هناك كلمات كثيرة مستحدثة في اللغة العربية نتيجة الترجمة من اللغات الأخرى، ونتيجة للتداخل الثقافي بين الأمم، والتواصل الحضاري بين الدول، مثل كلمة تلفزيون وراديو وغيرهما من الآلات، حتى كلمة "الإنترنت" شبكة المعلومات، وكل هذه المفردات ستكون غريبة على الباحث لو افتقد الحاسوب إلى جذرها، وذلك بالرغم من أن مجمع اللغة العربية أقرها وأخرجها في معجمه الوسيط، وكذلك الوجيز وأخبار إليها بالرموز المناسبة فنحن ما أشار إليها برمز

أما آن الألوان أن يكون هناك حاسوب عربي تكون اللغة العربية والأساس فيه؟

سؤال يبدو غريباً بعض الشيء على الحاضرين الآن؟ بل على كل المستفيدين من أبناء ومثقفين هذه الأمة، بالرغم من زعمهم لقيادة حركة الثقافة العربية؛ صحيح أن الحاسوب منتج غربي، وأساس برامجه وضع بلغة صانعيه، وهذا حقهم فهم الذين صنعوا ولابد من وضع لغتهم موضع الأساس في هذه الصناعة، ونحن المنتقمين علينا أن نلتزم بما صنعوا، ولكن إلى متى سنظل مستهلكين؟

لقد تمت محاولات في سبيل تذليل عقبات البحث في اللغة العربية عبر الحاسوب مثل تلك التي بدأتها الشركة العالمية صخر في بداية الثمانينيات وحتى عام 1985 وانصب معظمها على معالجة آيات القرآن الكريم ومعانيها وتركيب المفردات والجمل؛ المفردات من حيث تكوينها وصرفها أي استخراج المشتقات منها، ثم تركيب الجملة منها.

وبهذه المناسبة نقول أيضاً إن جهوداً كبيرة بذلت بعد ذلك وخاصة في ميدان الصرف الذي يعتمد بالدرجة الأولى على تكثيف البحث في الجذر اللغوي والمفردات المشتقة من هذا الجذر، وفي هذه المرحلة كما يقول

(1) رافقت الكمار ولبيلى السيد/ مقدمة عن الحاسوب ط. خاصة، 2003، ص 8.

اللغة العربية مثل أن الجملة تتكون من إما مبتدأ وخبره، أو من فعل وفاعل ومفعول وبالتالي فإن أي جملة تتوفر لها هذه الأركان هي صحيحة من وجهة نظر الحاسوب، فمثلاً إذا قلنا: أكل الرجل السماء، فإن هذه الجملة صحيحة نحويًا، ولكنها أسلوبياً ومعنوياً لا تصح، وبالتالي ستكون هناك مشكلة كبرى في المفرد والدلالة، ومن ثم يحتاج الأمر إلى تغذية الحاسوب ببرامج توضح الصحيح من غير الصحيح أسلوبياً فلا تكفي الصحة النحوية للجملة لتكون مقبولة، ولكن يجب إفادتها معنى صحيح حتى تكتمل لها صحتها.

وهذه المرحلة من المراحل المهمة في المعالجة الحاسوبية للغة العربية، وتحتاج إلى جهود كبيرة وبرامج متعددة لأنها ستساعد في تشكيل الجمل بشكل صحيح، وربما تساعد الباحث في معرفة ما يريد مرفقه، وسيكون في هذه المرحلة ما يسمى بـ (Meta Language) أو الميتا لغة التي يمكن عن طريقها تصنيف اللغة تصنيفاً هائلاً ومناسباً فترتبط أجزاء الجملة ببعضها برباط منطقي يقبله العقل وتقبله السليقة اللغوية.

وهذا يجزئنا إلى الحديث عن معضلة أخرى ثالثة، وهي الدلالة، حيث يفترض أن كل متحدث يعني دلالة من حديثه، وهذا يحتاج إلى معجم آخر يضاف إلى المعجم الأساسي الذي وضع على أساس الجذر، وهو ما يمكن أن نسميه بالمعجم الدلالي الذي يعني ببيان

«من» وتمني مولدة، و«د» أي دخيلة، و«مستحدثة» للكلمة المنقولة من لغة أخرى وصارت بالاستعمال كلمة مستخدمة عربياً، والسؤال أين توضع هذه الكلمة في الجذور؟ ولا بد من إيجاد مخرج لهذه المعضلة حتى يتمكن الباحث من العثور عليها بسهولة في إطار بحثه.

كانت هذه هي المعضلة الأولى والأساسية التي نهدف إلى الحديث عنها، ونتمنى أن يوجد لها مخرج، وهي عملية ليست باليسيرة على الخبراء في مجال البرامج الحاسوبية إذا أرادوا أن يضيفوا إلى جهودهم، ويضفوا عليه مزيداً من الدقة العلمية والبحثية.

وتتمثل المعضلة الثانية في اللغة العربية والبحث عنها في الحاسوب مشكلة التركيب أي تركيب الجملة، وهي ما يدخل في إطار علم النحو الباحث في كنهيات تركيب الجمل، ولأن الحاسوب أو الكمبيوتر آلة صماء كما يقول كمال بشر في بحثه في هذا الصدد «لا تمي ولا تفكر ولا تعقل إنه آلة تنفيذ، تعطي ما منحتها، وتقدم ما حشيت به من مادة سواء أكانت هذه المادة صحيحة أم غير صحيحة، دقيقة متكاملة أم غير ذلك، وهذا يفرض على المشتغلين بهذا الحقل مسؤولية الأمانة والدقة والكفاية العلمية»⁽²⁾ وفي هذا الشأن نرى أن الحاسوب الكمبيوتر أو برنامجه الذي وضع فيه، قد غذى بقواعد

(2) كمال بشر، صفحات من كتاب اللغة، ط غريب، 2004، 249.

والحقيقة أن هذا المجال مازالت الجهود فيه ناقصة وغير مكتملة، ونحن نعذر مصممي البرامج العربية على الحاسوب، لأن هذا الأمر يحتاج إلى تكوين مجموعات بحثية كبيرة تضم خبراء في المجالين؛ الخبراء في مجال الحاسوب، والخبراء اللغويون لتكتمل المنظومة، فمازالت الجهود تنسم بالفردية، ومهما كانت عيقرية الصمم لهذا البرنامج أو ذاك، فإن جهده لا بد أن يكمل ويتعصب في مرحلة من المراحل ومن ثم يتوقف، أما إذا كان العمل جماعياً فإنه بالتأكيد سيكون أفضل وأقرب إلى الاكتمال، وإن كنا نعي أن هذا يحتاج إلى دعم مادي ومالي ضخم، ولا بد أن يقوم القادرون مادياً ومالياً بدعم هذه الجهود، فليس بكثير على لغتنا التي هي عنوان هويتنا.

وهنا أنوه بمشروع يتم الإعداد له حالياً في مجمع اللغة العربية بالقاهرة، وهو مشروع المعجم التاريخي التي تسمى اللجنة المشكلة للتخطيط له وتنفيذه إلى البحث عن الدعم المادي له، وأعلن أن أحد الأمراء والمسؤولين في الإمارات العربية المتحدة سيقوم بدعمه، وتنمى أن يحذو حذوه بعض رجال المال والأعمال العرب الذين يملكون الملايين من العملات الأجنبية والعربية، لأن واحداً بنفسه مهما كانت قدرته على الدعم لن يستطيع الاستمرار في الدعم وحده، وذلك أمر لا بد أن تضعه اللجنة في الحسبان حتى لا

السجلات المختلفة لسلمفردة المشتقة من الجذور، وهنا يجب أن ننوه بالجهود المشكورة التي قامت بها الشركة العالمية (صخر) في هذا الصدد عند إعدادها لبرامج لغة القرآن ومعانيها، ولكن الأمر مازال يحتاج إلى مزيد من الجهد في هذا الصدد، لأن هناك نصوصاً أدبية أخرى شعرية ونثرية تشمل استخدامات متعددة للمفردات بجانب استخداماتها في القرآن الكريم.

وهذا يجزئنا إلى مسألة السياق ومقام المتحدث، فنحن حتى الآن حينما نهض في المعاجم التي وضعت على الحاسوب ربما نعرف معنى الكلمة الوضعي أي الذي وضعت له مع العلم بأن هذا ليس كافياً، لأننا سنكون في اضطراب حينما أجد اللغة أو المفردة التي أبحث عنها في سياق متأخر لهذا المعنى المعجمي الوضعي، فهل يمكن تصميم برامج تحمل هذه المعاجم التي تشير إلى المعاني المحتملة لسلمفردة في السياقات المختلفة، خاصة وأننا نعرف أن اللغة العربية لغة بلاغة وأدب، والأوائل الذين فكروا في المعاجم انطلقوا في رصد المفردات من خلال وجودها في هذه اللغة الأدبية البليغة في الشعر والنثر على السواء بجانب القرآن الكريم، وهم لم يخلعوا مفردات بل إنهم رصدوا لغة موجودة بالفعل داخل سياقاتها، حتى وإن بذلوا جهوداً كبيرة في تتبع المفردات في اللهجات واللهات التي يتكلمها أهل القبايل العربية المختلفة.

يجمع الباحثون والدارسون من مهندسين ولغويين على كلمة سواء واضحة الفكرة والتخطيط والهدف، سعياً إلى الوصول إلى غايتنا المنشودة المتمثلة في معالجة العربية بالحاسوب علاجاً علمياً متكاملًا، قابلاً للتطبيق العملي الشامل⁽³⁾.

وبالرغم من أنه يشهد بالجهد الذي قام به وما يزال يقوم به مركز القاهرة العلمي في سبيل إعداد أو وضع معجم عربي باستخدام الحاسوب إلا أنه يرى أن الأمر يحتاج إلى دعم مادي ومالي وعلمي بالإضافة إلى جهود جهات أخرى معنية بالأمر، وكذلك مراكز الحاسوب المختلفة حتى يتسنى إكمال المشروعات في الصورة التي ينبغي أن تكون عليها.

وعلى المستوى العلمي المتخصص فإنه يرى أن جهود المركز في إنشاء هذا المعجم على الحاسوب قامت على اتباع الخطوتين التاليتين ما:

1- تسجيل مادة الجذر المعين كاملة (قدر المستطاع).

2- تسجيل الخواص أو السمات المميزة لكل مادة بصيغها ومفرداتها المختلفة.

إلا أنه يرى أن المركز اعتمد على المجمعات الموجودة بالفعل، ومعظمها يشوبه بعض القصور في معالجة الجذور اللغوية لعدم

(3) كمال بشر، صفحات من كتف اللغة، ص 251.

يأتي وقت يكون العمل فيه على قدم وساق ثم يفاجأ المسؤولون بتوقف الدعم المالي لهم.

وبهذه المناسبة يمكن لخبراء الحاسوب أن يتفقوا مع القائمين على هذا الأمر على الدخول معهم بجدية في هذا المشروع عن طريق الحاسوب وهذا سيحقق فائدة على مستويين: الأول ضمان تسجيل المادة العلمية بدقة وأمان، فمسألة البحث بالبطاقات والتي كانت وما زالت مستخدمة في إعداد المعاجم، صارت قديمة وغير فعالة، لأنها تستغرق وقتاً وجهداً كبيرين، ولأنها عرضة للضياع والتلف وتسجيل المادة كمبيوترياً أو حاسوبياً سيضمن صمد ضياع هذه المادة العلمية أو تلفها، وسيضمن سرعة الإنجاز إلى حد كبير. أما المستوى الثاني، فهو اختصار المسافة، فبدلاً من الانتظار حتى يتم إنجاز العمل ثم نقوم بتسجيله في برامج على الحاسوب، فإن المادة ستكون مسجلة بالفعل ولن يحتاج الأمر إلى جهود أخرى ووقت آخر لتسجيلها، وبالتالي نضمن وجودها، ولن يحتاج الأمر بعد ذلك إلا تنظيمها في برامج وتسهيلها على الدارسين.

واللافت للنظر أن رئيس هذه الهيئة وهذه المجموعة المشكلة للإعداد للمعجم التاريخي وإنجازه هو الدكتور كمال بشر نائب رئيس مجمع اللغة العربية، وأحد اللغويين العظام في هذا العصر، وهو الذي دعا في محاضرة له نشرت ضمن كتابه صفحات من اللغة التي أشرت إليه من قبل إلى "إنشاء مركز قومي

ثالثة وجب كتابتها ألفاً إذا كان أصلها الواو
 وماء إذا كان أصلها الياء أما إذا كانت همزة
 أصلية مثل قرأ فإنها تظل على حالها.
 وفيما يخص مد حرف- في الكتابة فقط-
 وذلك مثل: كتبوا فهل يجوز مد الكاف
 لتكون هكذا: "كتبوا"، أو مد الراء لتكون
 هكذا "كتيروا" أو مد الباء لتكون هكذا
 "كتبوا" وهو أمر يقع في لبس لأن السين
 صارت في الكتابة الرقمة تكتب بدون الأسنان
 الثلاثة (س) التي كانت مستخدمة في الكتابة
 القديمة والحديثة أيضاً.
 وفي النهاية لابد أن نحفي الجهود العظيمة
 والبحوث المقدمة في طرح معضلات البحث في
 اللغة العربية على الحاسوب، وما زال يحدونا
 الأصل في التعريب الكامل لهذه الآلة التي
 صارت تلعب دوراً مهماً وخطيراً في حياتنا،
 ولا بد من تيسيرها أمام الباحثين في اللغة
 العربية، ولعل تذليل العقبات والصعوبات
 التي تعترضها تساعد على إعادة الهبة
 المفقودة للغة العربية بين أبنائها.

حرص بعض هذه المعجمات على إكمال مادة
 الجذر في أحيان كثيرة ويضرب مثلاً "بلسان
 العرب" وهو ما هو في طبيعته وهدفه وحجمه
 "كثيراً ما يهمل بعض الصيغ أو المفردات،
 وينحوه بدلاً من ذلك- مخاخي أخرى تتصل
 بالثقافة العامة أو الأدب أو التاريخ"⁴.

وتمثل مسألة الكتابة على الحاسوب معضلة
 أخرى أمام الباحثين في اللغة العربية على
 الحاسوب، وكثيراً ما نلاحظ في الكتابة عليه
 ظهور الحرف الخطأ بخط أحمر، والذي
 يعني خطأ، وبالطبع ناتج عن تغذية
 الحاسوب بطريقة كتابية معينة خاصة في
 الياء المهملة والمنقوطة، هذا بالإضافة إلى
 المعضلة الأساسية وهي الوحدات الكتابية
 للحروف العربية؛ فستغذية الحاسوب
 بالوحدات الكتابية وصورها المنوعة يقتضي
 حرصاً فائقاً ودقة كاملة في التصنيف والتفريق
 وبين الخواص المميزة لكل وحدة وكل صورة
 وبخاصة أن كثيراً من رموز الكتابة العربية
 متشابهة أو متماثل وذلك يظهر أكثر في النقاط
 وعديه، فقد تنحرف النقاط عن موضعها
 فتحدث لبساً ومن ثم يكون الخطأ.

وكذلك مسألة، الكلمات أو الأفعال التي
 تنتهي بالفاء منقلبة عن أصل هو الياء أو
 الواو، وإن كان مركز القاهرة العلمي قد حقق
 فيها إنجازاً إلا أن الأمر يحتاج إلى مزيد من
 التبسيط، فالتقاعدة تقول: إذا وقعت الألف

(4) كمال بشر، المرجع السابق، ص 256.

واحة مكتبات نت

أ.عبيد أحمد

blroonlmed@hotmail.com

حكمة العبد:

تستغرق مناقشة المسائل الثقافية وقتاً طويلاً ...
لأن بعضنا يعرف عنها أكثر مما يعرف عن المسائل الهامة.

علماء العرب

هو أبو الحسن علاء الدين علي بن أبي الحزم

العرفوف بأبن النفيس، وأحياناً بالقرشي نسبة إلى قرش، في ما وراء النهر، ومنها أصله. وهو طبيب وعالم وفيلسوف، ولد بدمشق سنة 607 هـ وتوفي بالقاهرة سنة 687 هـ. درس الطب في دمشق على مشاهير العلماء، وخصوصاً على مذهب الدين الدخوار. ثم نزل مصر ومارس الطب في المستشفى الناصري، ثم في المستشفى المنصوري الذي أنشأه السلطان قلاوون. وأصبح عميد أطباء هذا المستشفى. وطبيب السلطان بهبرس، وكان يحضر مجلسه في داره جماعة من الأمراء وأكابر الأطباء. قيل في وصفه أنه كان شهجاً طويلاً، أسهل الخدين، نحيفاً، ذا مروءة. وكان قد اهتم داراً بالقاهرة، وفرشها بالرخام حتى ابوانتها. ولم يكن متزوجاً فأوقف داره وكتبه وكل ما له على البيمارستان المنصوري.

لم تقتصر شهرة ابن النفيس على الطب، بل كان يعد من كبار علماء عصره في اللغة، والفلسفة، والفقه، والحديث. وله كتب في شبر المواضيع الطبية، منها: الرسالة الكاملة في السيرة النبوية، وكتاب فاضل بن ناطق، الذي جارى في كتاب (حي بن يقظان) لابن طفيل، ولكن بطريقة لاهوتية لا فلسفية.

كلمات لها معنى

- ❖ إن الحب يفلسنا من الحقد .
- ❖ إن كلمات الحب أجمل من الحب .
- ❖ الحب يولد من لا شيء .. ويموت بأي شيء.
- ❖ الحب ليس لوناً واحداً ولكنه كل الألوان.
- ❖ الذي يحب يصدق كل شيء أو لا يصدق أي شيء .
- ❖ الإهمال يقتل الحب، والنسيان يذقنه .

استمارة اشتراك في مكبات IPISCOM

نوع الاشتراك: مؤسسات ☐ أفراد ☐

الاسم (اشترك الأفراد):

الوظيفة:

اسم الجهة (اشترك المؤسسات):

العنوان البريدي ص.ب:

رمز بريدي :

المدينة :

الدولة:

ت :

ف :

بريد إلكتروني:

عدد النسخ: أرغب/الاشتراك في عدد ☐ نسخة

التوقيع

استمارة اشتراك في مكبات نت

عليك أن تملأ استمارة الاشتراك المرفقة وفقاً للتالي:

- الاشتراك للأفراد من داخل جمهورية مصر العربية بمبلغ 100 جنيهًا مصريًا في العام نقداً لندوبنا أو بالحضور في مقر الشركة أو بحالة بريدية أو بشيك مصري باسم شركة "إيبيس.كوم للنشر والتوزيع وخدمات المعلومات"
- الاشتراك للمؤسسات من داخل جمهورية مصر العربية بمبلغ 220 جنيهًا مصريًا في العام نقداً أو بشيك مصري باسم شركة "إيبيس.كوم للنشر والتوزيع وخدمات المعلومات"
- الاشتراك للأفراد من الدول العربية بمبلغ 35 دولاراً في العام نقداً أو بشيك مصري باسم شركة "إيبيس.كوم للنشر والتوزيع وخدمات المعلومات"
- الاشتراك للمؤسسات من الدول العربية بمبلغ 70 دولاراً في العام نقداً أو بشيك مصري باسم شركة "إيبيس.كوم للنشر والتوزيع وخدمات المعلومات"
- الاشتراك للأفراد من أمريكا وأوروبا بمبلغ 45 دولاراً في العام نقداً أو بشيك مصري باسم شركة "إيبيس.كوم للنشر والتوزيع وخدمات المعلومات"
- الاشتراك للمؤسسات من أمريكا وأوروبا بمبلغ 90 دولاراً في العام نقداً أو بشيك مصري باسم شركة "إيبيس.كوم للنشر والتوزيع وخدمات المعلومات"

يمكنك أيضاً القيام بتحويل بنكي على حسابنا في البنك المصري الخليجي فرع الجيزة رقم 303372 جمهورية مصر العربية. يسعدنا دائماً في IPISCOM من خلال مكاتبنا. نت أن نستقبل اقتراحاتكم، ولا نستطيع أن نقول في نهاية رسالتنا المفتوحة إليكم إلا أهلاً بكم في مستقبل المكاتب والمعلومات في العالم العربي.

يمكنك الحصول على أعداد دورية مكاتب نت مجلدة.

ترسل كافة المراسلات باسم

رئيس التحرير

د. زين عبد الهادي

ص.ب 647 الأورمان - الرمز البريدي 12612 الجيزة جمهورية مصر العربية

IPISCOM

مكاتب نت

توزيع شركة إيبيس كوم للنشر والتوزيع وخدمات المعلومات

رقم الإيداع: 2002/12102

91-
om www.
ipisegypt.com www.ipi-
pt.com www.ipisegypt.com ww
n.ipisegypt.com www.ipisegypt.c
gypt.com www.ipisegypt.com
www.ipisegypt.com www.ipisegy
pisegypt.com www.ipisegypt.co
www.ipisegypt.com www.ipise
n.ipisegypt.com www.ipisegypt
om www.ipisegypt.com www.i
ipisegypt.com www.ipisegy
ipisegypt.com www.ipi

منه! علانك هنا

අප. ඔබ!

للنشر والتوزيع وخدمات المعلومات

دراسات

مَلَاوِي

دوريات

کتاب

حول الشركة

[illegible]

على أيدي مجموعة من الخبراء العرب في مجال تخصص المكتبات والمعلومات تأسست شركة إيبيس. كوم في ديسمبر من عام ١٩٩٩ بهدف نشر وتعمية الوعي الفكري في مجال المكتبات والمعلومات بين المتخصصين والمهتمين بهذا المجال وتطبيق تكنولوجيا المعلومات ونشر ثقافة الإنترنت والمكتبات الرقمية.

وتقدم الشركة مجموعة من خدمات المعلومات تتمثل في مايلي:

١- البحث في قواعد البيانات الأجنبية .

٢- البحث على شبكة المعلومات الدولية الإنترنت .

٣- تصوير وتسليم المقالات المتاحة في الدوريات المصرية.

٤- البحث عن الكتب المصرية وشحنها.

٥- البحث عن الرسائل الجامعية المتاحة من الجامعات المصرية.

٦- تسهيل الحصول على أى مصدر معلومات نشر في مصر .

٧- تسهيل الاشتراك في مؤتمرات وندوات المعلومات وتكنولوجيا

المعلومات المنعقدة في مصر.

٨- تيسيل الحصول على مصادر المعلومات من معارض الكتب في

مصر وشحنها.

اسم المستخدم:	
كلمة المرو:	
دخول	
انت الزائر 67696	

© ٢٠٠٨ - ٢٠٠٠ كوم إيبيس. جميع الحقوق محفوظة لشركة إيبيس